Joint Committee on the Draft Investigatory Powers Bill

Oral evidence

Rachel Logan, Law and Human Rights Programme Director, Amnesty International (QQ 197-206)

Evidence heard in public Questions 197-206

Oral Evidence

Taken before the Joint Committee

on Monday 21 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Suella Fernandes MP, David Hanson MP, Shabana Mahmood MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Lord Hart of Chilton, and Lord Strasburger.

Witness: **Rachel Logan**, Law and Human Rights Programme Director, Amnesty International, gave evidence.

Q197 The Chairman: A very warm welcome to all three of you. Thank you so much for coming along so close to Christmas. We are very grateful. As you probably know, the way the Committee operates is that we will ask you a number questions, which we hope will give you the opportunity to make whatever points you want. I will open by asking you a very general question and in each of your replies please feel free to make anything you like by way of an opening statement. What do you think of the draft Bill? Do you think it strikes the right balance between safeguarding our civil liberties and crime prevention? Perhaps we can start with you, Ms Griffin.

Rachel Griffin: I should start by saying that I am from the Suzy Lamplugh Trust. We run the National Stalking Helpline. A large proportion of the people who we help each year are affected by digitally-assisted stalking of some kind or another. The first thing to say about the draft Bill is that it is definitely necessary, from our point of view, for the police to have access to communications data to investigate many cases of stalking and cyberstalking. It is certainly necessary for the police to be able to access communications data to investigate and detect crimes. However, the point we want to make is that legislation should be only one part of a strategic plan to address digital offending. On a day-to-day basis we are finding that the police often do not make very good use of the legislation that they already have available to them. Our question would be whether a change in legislation would have an impact on the experience of victims on a day-to-day basis. On whether the Bill strikes the right balance between safeguarding and civil liberties, I defer to other organisations to answer that question. Our point of view is very much on the experience of victims of stalking.

The Chairman: That is what we would expect it to be.

Rachel Logan: Amnesty very much welcomes the opportunity to be here. We very much welcome having a draft Bill of some kind, because we are one of those organisations that has been saying for a long time that the existing statutory framework in this area is not up to scratch. Unfortunately, we are very disappointed by what we see in the Bill that has been

put forward. To touch on a very small number of areas, given the time available, first, we see in the Bill not one, not two, but five sections dealing with bulk, indiscriminate collection of or interference with individual privacy. From our perspective, that simply does not strike the balance or draw the line in the right place. We even see some targeted powers shading into what we would see as bulk powers in the case of thematic warrants.

I move on to intelligence sharing, which we have been litigating on for more than 18 months in the Investigatory Powers Tribunal. It has been the subject of at least two rulings. We were very surprised to see in what bare terms it is dealt with in the Bill, given how big the subject area is. We would have liked to have seen a clear, accessible framework, dealing with how material is received and sent overseas outside the MLATs. We would have liked to have seen that limit and not include the product of bulk interception either way—going from the UK or coming into the UK.

On oversight and judicial authorisation, unfortunately, we are disappointed by the judicial authorisation, or judicial review process, as it is put in the draft Bill. It does not amount to proper, independent judicial authorisation as is required for human rights compliance. It is simply not there. On the oversight provisions, similarly, having been through the IPT—I hope that I will get the opportunity to expand on this—we are very disappointed to see only one real substantive change to the way the Investigatory Powers Tribunal does its job. We would have liked to have seen a much more thorough look at how that works and whether it is properly independent and effective.

Finally, to touch on special protections in the Bill, again, this is an area that Amnesty has been litigating on in terms of legal professional privilege in the Investigatory Powers Tribunal, where we saw a concession by the Government that their entire regime in this area had not been human rights compliant. We saw a further finding that one of our co-claimants' legally professionally privileged material had been unlawfully retained. It is very disappointing to see nothing on the face of the Bill to deal with that properly, to deal with journalists, or even to consider giving further protections to human rights NGOs, such as ourselves, who we now know have, disappointingly, been specifically targeted for surveillance by the state. With all of that in mind, and there are many other areas that we simply do not have time to get into at this stage with the time allowed for the Bill process, we are very disappointed with what we have been presented with.

The Chairman: Thank you very much. Of course, every organisation, including yours, is very much entitled and welcomed by us to submit written evidence in detail.

Rachel Logan: We have done, this morning, for which we are grateful.

Alan Wardle: Good afternoon. Another fact that is relevant for this is that the NSPCC runs ChildLine, which you will all be aware of. It is now in its 30th year. Increasingly, children, as the Committee will know, are leading their lives online. More than three-quarters of 12 to 15 year-olds have access to a smartphone. That also means that many of the crimes committed against children increasingly have an online element. In particular, some of the ones I want to focus on are what you might call the harder-end cases, such as the possession, distribution and manufacturing of child abuse images, so-called child pornography, which is growing, and also cases of grooming of children, much of which is

done online. More than 500 children contacted ChildLine last year about grooming and more than 80% of those cases had an online element to it.

From our perspective on the Bill, the most important thing for us is to ensure that the police have the powers that they need to track, investigate and prosecute these offenders. We are coming from a different place from Amnesty, which is more about bulk surveillance; we are more focused on specific criminal investigations that the police need to undertake. We have a particular concern that Clause 47 might be restricting too much the police's ability to investigate in what can be quite complex investigations.

Another point I want to make is that ChildLine has a very high level of confidentiality, but it has to breach children's confidentiality around 10 times a day, generally because those children are actively suicidal. Most children contact ChildLine online these days, so we need to ensure police can get those IP addresses quickly and actively intervene to protect those children. The two aspects that I would like to talk about are criminal investigations and ensuring police have powers, and an emergency function to protect a child's life if they are in immediate danger.

The Chairman: Thank you, all three of you, very much indeed for those opening remarks.

Q198 **Mr David Hanson:** The police's case, as put to us by Keith Bristow of the National Crime Agency, is that the Bill brings us up to speed with "what we need to be able to do in a digital age compared to an analogue age". Do you agree with that, or do you think the Bill goes further and adds new powers for the police?

Rachel Griffin: I smiled because I can see why that statement was made in theory, and it might well apply to cases of, for example, child sexual exploitation, where the focus is on intervention and stopping criminal activity escalating. From a stalking point of view, the key use of communications data in cases that we deal with is on investigation and detection in individual cases where the activity has already happened. We tend to find that it is not so much a case of whether the police have the powers; they already have a number of powers but we find that they simply are not being used in practice. For example, we often hear from victims of stalking who have been told to turn off their computer—"If you don't look at the emails it won't affect you"—or they might be told that that it is too expensive to investigate digitally, or that there is no point as the service providers will not be compliant, et cetera. For example, recently the helpline report was told that police access phone records only in cases of murder. There is a huge gap between what is going on in practice with regard to making use of existing powers and what may be envisaged in terms of the potential of the Bill. That is why we would like to see the police using their current powers to full capacity, as is reasonable and proportionate, but also to focus on not just legislation but the capability and capacity of police forces to make use of that legislation.

Rachel Logan: I will leave this to my colleagues at this stage.

Alan Wardle: The police's view on powers is quite important. From our perspective, we understand from the NCA that there has been a gradual erosion of the amount of data that they have been able to gather over the years. The Bill is very important to put that in place and to ensure that it is adaptable. Who knows what technologies there will be in five to 10 years' time, but the Bill has to have sufficient flexibility to adapt to those things.

On Clause 47(4), which has additional restrictions on granting authorisation, we have had initial conversations with the police and they have expressed concern about it. It would seem to us perverse if the data providers were able to hold all the information but the police were unable to access it. My understanding is that if people were conspiring over the telephone the police would be able to have all that information, but not if it was done online. That subsection talks about where the activity is mainly or wholly acquiring material the possession of which is a crime. Something such as possessing child abuse images is clearly a crime, but we know that for grooming cases where a lot of people are involved and it takes a long period of time, where, for example, a person books a hire car in place A and drives to place B or they book a flight, those factual issues, while not a crime in themselves, can help the police to investigate. It would be worrying to us if anything restricted the police's ability to investigate thoroughly along all the different strands of investigations. We would want to ensure that there is parity across the board and that the data the providers hold can be accessed by the police force for specific investigations.

Mr David Hanson: The question to all of you is: are the police powers under existing legislation proportionate and effective? Will they be more proportionate and effective under the proposed Bill, or will they be neutral or less effective? What is your view as to the police-central cases: do we need the Bill to update what we currently do? Is that right?

Alan Wardle: Yes it is, but my understanding is that this clause in particular would place a restriction on them that is not currently there. That would need to be worked through to see why it has been put in there and whether it will actively hinder the police's investigation of the kind of complex cases that I am talking about: the production of child abuse images, which, again, are quite often done by conspiracies, and online grooming. Yes, the need to have these additional powers is quite clear.

Rachel Logan: I am afraid that the question of police powers is not something that Amnesty can assist the Committee with at this point. It is not a part of the Bill that we have assessed or been involved with to date.

Mr David Hanson: With due respect I think that that is copping out of an answer. If the Bill goes forward, is Amnesty satisfied that the current proposals by the police are modernising their view based on the Bill? Ultimately it is about police powers and whether they are effective and proportionate. Surely Amnesty has a view on that.

Rachel Logan: With respect, it may be seen as copping out, but we are talking about a Bill of many hundreds of pages and many parts. Amnesty is a worldwide movement that focuses on many different aspects. We simply have not assessed those parts of the Bill yet.

Mr David Hanson: So you do not have a view on whether these current proposals are proportionate and effective.

Rachel Logan: At this point I do not have a view that I can assist the Committee with on the police powers in those parts of the Bill. I can help you, as much as Amnesty can, with questions of necessity and proportionality around bulk interception warrants, the structures around targeted warrants, and what is in the Bill on intelligence sharing, but I am afraid that the question of police powers and dealing with crime simply is not something I can help you with.

Mr David Hanson: Ultimately those are police powers. The question is whether they are proportionate and effective in relation to what the Bill proposes.

Rachel Logan: I am afraid that this simply is not something that we can assist you with. Those parts of the Bill go into Parts 3, 4 and 5. There are multiple parts of the Bill. We have not had a significant amount of time and they are not core areas of focus for us at this point.

Mr David Hanson: May I respectfully suggest that, when the Bill comes before both Houses of Parliament we would want a view on those issues? They are central to the Bill.

Rachel Logan: It may well be that, when we have had considerably more time and when the Bill goes through the proper processes, we will turn to that. I simply cannot say at this stage whether that will be Amnesty's focus.

Rachel Griffin: Our view is that it is unlikely—or that we are yet to be convinced—that the Bill will have an impact on the majority of cases of stalking as we experience them. That is not because data communications are not needed, but because the expertise in digital investigation and recognising risk is not as widespread in day-to-day policing as it needs to be.

Q199 Suella Fernandes: This is a question to Rachel Griffin and Alan. Can you walk us through a typical harassment case—if there is such a thing—or a child sexual exploitation or a grooming case, and how communications data would be helpful in identifying perpetrators and securing a conviction?

Rachel Griffin: From a stalking point of view, around 70% of people who call the National Stalking Helpline report experiencing at least one form of stalking behaviour that may require police to access some kind of communications data. Some 39% have received phone calls; 30% have received emails; 36% have received texts; and 37% have experienced stalking via some kind of social networking site. It is right that you made the point that there may not be a typical case of stalking because each one would be quite different. They are incredibly diverse in how long the stalking goes on for; some will be stalked for about six months, but, sadly, we have a small proportion of people who have been stalked for a number of years.

What tends to happen is that somebody will be stalked through a blend of different means. That may include physically turning up at someone's workplace or at their home, perhaps sending them letters, but also saying things about them via social media. Some will know that they are being stalked and that the activity is taking place online, but they do not necessarily know who it is, or there is a suspect but it is very difficult for them to prove. They will go to the police and say, "This has been happening, I've been receiving these text messages, these things have been written about me on Twitter". In a case where there may have been a number of text messages or emails, the police may need to identify that it was in fact a perpetrator—an identified individual—who sent them. That is where communications data may come in. Unfortunately, that is where we have too many examples of victims saying that they have gone to the police and found that, in some cases, the police do not even understand what an IP address is. The level of understanding is relatively low. That is alongside those cases where people say, "Well, come back when he

does something", suggesting that if it happens on the internet—if the stalking is cyberstalking—it is not real stalking.

Alan Wardle: It varies in grooming. Sometimes it can be one person grooming one child, or, as we have seen in some high-profile cases, it can be gangs of people communicating with several children. The process of grooming takes time, by its very nature. It lures children in, makes them feel good about themselves, offers them enticements, et cetera. We know from the National Crime Agency that the vast majority of cases involving grooming are online. That could be through social media, by various apps, by text message, by phone et cetera. Quite often, one of the challenging things around this is that children do not even recognise that they are being groomed—they think that it is their boyfriend, for example. The child will not necessarily keep the evidence themselves; they will not hold on to it. The police need to be able to identify from all those different sources what happened, to try to get a picture of who said what to who, where they were, who they communicated with, when they did it, et cetera, to build up a picture of what is going on, which obviously would go alongside personal testimony. That is why the point that Rachel Griffin makes is valid: we also have concerns about the police's capability—particularly that of local forces—to investigate and understand these offences properly. The cornerstone to that is having the information available to them so that they can identify what has happened, build up a picture of what is going on and investigate and prosecute these crimes.

Q200 **Baroness Browning:** Are the three purposes for which law enforcement can seek internet communication records the right ones? Should they also be able to use them for other purposes—for instance to locate missing people—even when no crime is suspected? We have received evidence from the police that much of their time is taken up with trying to identify vulnerable people, not necessarily because they have fallen foul of serious crime, but speed is of the essence because they are vulnerable.

Alan Wardle: On the first part of your question, as I mentioned, certainly on Clause 47(4)(c), which is the limitation where a person is "making available, or acquiring, material whose possession is a crime"; at first glance, and having had an initial discussion with the NCA, we are concerned that that might be too limiting. Using grooming as an example again, hiring a car to transport a child from one part of the country to another is not a crime in and of itself, but it is evidence of a crime having taken place. It would be worrying to us if that data was held by internet service providers but the police could not access it because it was not illegal material. More needs to be teased out throughout the process about what that means and what limitations that will place on the police.

On the emergency bit, as I said, ChildLine has to do this about 10 times a day. We work with CEOP very closely. The ability of the police to identify and rescue actively suicidal children who may not want to be contacted by the police is a very important function. We certainly would want to ensure that that capability is not eroded in any way.

Baroness Browning: Not eroded, but as drafted, will it not add anything to resolve the problem of your 10 children a day?

Alan Wardle: I spoke to a barrister about this last week. Her initial view was that Clause 46(7)(g), "for the purpose, in an emergency, of preventing death or injury or any damage

to a person's physical or mental health", would cover this situation, but again, it would be useful for the Home Office to clarify whether, in its view, that would cover it.

Q201 Lord Strasburger: Ms Logan, you mentioned in your opening remarks that one of the five areas you are concerned about is intelligence sharing. There is very little in the Bill about it and so far the Committee has heard very little about it. Would you care to expand on what Amnesty's concerns are and what advice you would give the Committee on it?

Rachel Logan: Yes, thank you very much. Amnesty has been engaged, together with Liberty, Privacy International and several other NGOs, in litigation in the Investigatory Powers Tribunal—it will now be off in the European Court of Human Rights in Strasbourg on this subject—to look at the way the UK both sends information, intelligence product, overseas and receives it from overseas powers. In the Bill we have very little at all on what are called "overseas arrangements". Clause 39, "Interception in accordance with overseas requests", provides for that activity, but simply talks about lawful interception being something, "carried out in response to a request made in accordance with a relevant international agreement by the competent authorities of a country or territory outside the United Kingdom". The only definition you have for a "relevant international agreement" is, "an international agreement to which the United Kingdom is a party". On the other side of the coin, when we think about what the UK is requesting others to do—perhaps not requesting, but what information it might receive from other powers—all we have in the Bill is a bare reference in Schedule 6 to a "code of practice", which, it is said, will be forthcoming and which will deal with the "provision about the making of requests ('relevant overseas requests') for intercepted material or related communications data that has been obtained by an overseas authority by means of any interception", et cetera, with no definitions of what any of this might be and no expansion on what any of this might mean. There is then further provision for arrangements to be in place around receipt or sending of such information, with no explanation of whether such arrangements will be public, what they might contain or what they might be.

We were talking about the product of bulk interception, such as, in the US, the product of Prism or the upstream programmes where material has been collected in bulk. We are considering a situation where we have a ruling in the Investigatory Powers Tribunal case that recognises that, until this litigation, any such intelligence sharing was unlawful because there was no policy whatsoever in the public eye in this area. All we got during the litigation was a small summary, which was corrected on many occasions, of what the arrangements in place might be. It was very bare bones. There was lots of talk about signposting to what was under the waterline. When we were in that situation we had very much expected the Bill, in the spirit of transparency, to provide a clear legal framework. Those simple references simply do not do that. How can Parliament and the oversight bodies provide proper scrutiny? How can the public understand where their information might end up or what might be being looked at overseas if there is simply nothing there? That is very disappointing.

The Chairman: I think we will touch on that in further questions as well.

Q202 Dr Andrew Murrison: Amnesty obviously has an international perspective. I am interested in your view on whether this legislation is compatible with the direction of travel

taken by countries with which we can reasonably be compared, in particular the other four members of the "Five Eyes" community.

Rachel Logan: I want to be very careful about what I say on that topic at this point because there is a certain state of flux in the relevant "Five Eyes" countries. I would be very happy to come back to the Committee with a more detailed analysis. I will say that in the US, for example, we have recently seen, as I am sure you are aware, changes around the Patriot Act and the Freedom Act and a certain amount of rolling back, but I would not want to give the Committee any precise answers without being able to go back to that in more detail. I would be happy to do so.

Dr Andrew Murrison: It would be quite valuable if you could as part of written evidence. As we have been going through this there have been comparisons with the "Five Eyes" community, with whom, of course, we share data. It would be useful from your perspective as an international organisation to provide some insights if you could.

Rachel Logan: I will certainly see whether we can do that in the time available.

Dr Andrew Murrison: Thank you very much. May I ask you about communications data? A lot of what we have been dealing with over the past few weeks has to do with the times permitted by the Bill—for example, five days for judicial review warrants issued by the Home Secretary and 12 months for the retention of communications data. I would be interested in your thoughts on whether 12 months is right—in particular, to nuance that slightly, whether that 12 months might be amended upwards or downwards depending on the situation, on the crime that we think has been committed and on the circumstances, thinking of missing people, for example.

Rachel Griffin: We would resist offering an arbitrary time limit, which I dare say is not terribly helpful. From the National Stalking Helpline's perspective, we tend to talk to people at the very beginning of their journey through the criminal justice system. They may not even have reported the crime when they talk to us. I would advise getting evidence from people such as the CPS and the police on how long it takes for a prosecution to come to court from that point of first report. That will have an impact. It will not be terribly helpful to have a time limit that may have expired when the evidence is finally gathered and a prosecution is pursued.

Also, it is worth bearing in mind how long people have been stalked for. Some 48% of the people who talked to us have been stalked for longer than one year. That suggests that there might be a need, by the time a victim goes to the police, to go back some time to find some of the essential data. It is also really important to understand why people do not come forward, whether it is to do with cyberstalking, or, in the context of stalking, things such as revenge porn. Often people will not come forward because they do not feel that they will believed and they do not have the confidence to talk about their experiences.

Also, it is vital to point out that, in preparation for this session, we contacted the Home Office to ask how many investigations are impacted by lack of communications data—we do not know what we do not know. The feedback was that it is impossible to know how many criminal investigations are impacted by a lack of available communications data. Again, I come back to the point that we definitely recognise the need for communications

data, but we do not know the size of the problem that we are trying to solve with the Bill. Therefore, it is difficult to determine whether the existence of the data would be helpful and for how long that data would need to be kept because we do not know how many prosecutions are not going forward without that data. It feels very circular.

Dr Andrew Murrison: Where do you think the Home Office got the figure of 12 months from, then?

Rachel Griffin: I am not sure. You would have to ask the Home Office.

Alan Wardle: My understanding of the 12 months was that the last time this was legislated for Parliament took the view that that was the appropriate time. Any flexibility around that ought to be evidence-led. Certainly, we know that some of the more complex cases, some of which I have alluded to, take a long time to build up the case. We hear from the police of cases where, because it is a rigid 12 months, as the case proceeds bits of evidence fall off the end after a year. We need to know whether there is any flexibility around that once a case has started. On disclosure, again, similar to the point that Rachel made, not all children disclose immediately whether they have been abused. They can take time. It is a judgment for Parliament to make. It ought to be evidence-led and take a view on whether there are more serious and complex crimes where data need to be held for longer and how that would work.

Dr Andrew Murrison: I can see why organisations such as Suzy Lamplugh Trust and the NSPCC should want the police to have these powers since you are faced, on a day-to-day basis, with very vulnerable people. However, do you have any concerns more broadly about the acquisition and storage of communications data and potential misuse of that material?

Alan Wardle: Yes. It clearly needs to be kept safe. Another thing to remember is that children are users of data as well and they will want to have their rights and privileges protected. Clearly, there have to be very strong safeguards around that. I am not a technical expert so I would not be able to tell you how that is done, but the data needs to be kept securely. It needs to be accessed in very strict conditions to give people confidence and assurance that the data is being used properly.

Rachel Griffin: I echo that. There will be a number of cases where someone who has been stalked will have their security, whether physical or online, compromised in some way. It is critical that they have confidence that their data will be treated appropriately.

Dr Andrew Murrison: In situations such as that of TalkTalk, are you confident that there are likely to be systems in place to guarantee people's safety and security?

Rachel Griffin: Guaranteeing safety and security is very difficult. It is particularly difficult when someone is motivated by the kind of obsession and fixation that stalkers commonly display. It would be completely wrong for me to say that I would have confidence that that can be guaranteed, but victims should have a reasonable expectation that their data will be kept as securely as possible.

Q203 Lord Hart of Chilton: I must disclose to the record that 50 years ago at university I joined Amnesty International.

The Chairman: You have disclosed your age as well.

Lord Hart of Chilton: I know—how youthful I still look. We have been supplied with the open determination of the Investigatory Powers Tribunal on 22 June 2015, from which we see that GCHQ retained material for longer than permitted under the policies. Therefore, there was a breach. My first question is whether, in the light of that decision, you are confident that there are sufficient safeguards in place governing the activities of the intelligence and security agencies. I rather think from what you said at the opening that you are not.

Rachel Logan: No, indeed. First, it is important to think about what that finding tells us and then look at whether we feel that the safeguards are sufficient in the light of that. It is important to understand that Amnesty found very little out from that determination. I can come back to the question of how we got it, which sheds rather a lot of light on our views on the Investigatory Powers Tribunal, but it tells us very little at all. We do not know why our communications were intercepted and selected for examination. We do not know what was looked at and when. We do not know what policy was breached or in what way. We do not know whether this was a one-off and just confined to us, or whether it is systemic among other NGOs that were not involved in the litigation. We have had no ability whatsoever to input into the conclusions of the tribunal because we were excluded from the hearing that resulted in that determination. That begs the much more important question, as far as we are concerned, which is why human rights NGOs were being targeted for surveillance in the first place, quite aside from whether our material was retained for too long. The other NGOs in the same legal action received a simple one line, "No determination in your favour", which does not tell them whether they were intercepted, or whether they were intercepted but the tribunal considered it to be lawful, et cetera.

It is a very sparse determination, but what that tells us about the safeguards and the oversight system is that something has gone very badly wrong. It appears that this has been considered an acceptable activity by the Secretary of State and all those others involved in oversight during the process, because we know that we were picked up under a general warrant. It appears that this is something that was carrying on which either nobody raised any objection to because they all thought it was fine and dandy to be spying on human rights NGOs and did not know about the specific policy breach, or they knew about the breach and did not consider it to be important. We do not know why this was not picked up until we got into a tribunal process. It is very worrying that we had to get to that stage to get this finding.

The same applies to the other litigation we have been involved in—the legal professional privilege one I alluded to earlier—where one of our co-claimants found that his legally privileged communications had been picked up. That is a really frightening proposition for those of us who have been involved in the legal system for a long time. Again, he was not able to contribute to the hearing where the finding was made that this was not very important. From our perspective, something needed to change with that in mind. We have not seen that something in the draft Bill, particularly if you look at the retention provisions in it. Data can be retained as long as it is necessary or "likely to become necessary" to retain it. That is stunningly broad. It is very worrying for us, having been in the position of having had our data retained and having been spied on, that we do not have more safeguards in

this. I can come on to look at the IPT and the judicial relation if you would find it helpful, but basically, against that background, there does not seem to be enough.

Lord Hart of Chilton: What further safeguards do you think are necessary?

Rachel Logan: It comes back to the question of definitions. There are incredibly broad definitions around purposes in the various warrants. There is no definition of national security. Just recently, a decision by the Grand Chamber in Strasbourg, I think last week, said that it is important to have tighter definitions than just "threats to national security" when we talk about warrants of this kind. You have these very broad definitions and general purposes permitted as a basis of interception. Then you again have a complete absence of proper judicial authorisation. In Amnesty's view, this so-called double lock does not amount to a human-rights-compatible process. The decision is still being taken by the Secretary of State. It is merely being reviewed on judicial review principles by a judicial commissioner. If Clause 19(2), which states that this must be done to a judicial review standard, was not intended in any way to limit the scope of the review undertaken by the judicial commissioner, then it is unnecessary or unnecessarily complicating the situation.

Our view—like, I am sure, many of the other NGOs you have heard or will hear from—is that that is simply unnecessary if the intent is to have a full, merits-based review by an independent judicial authority before a warrant can be issued. We would like to see that happen. We would like to see strong post facto oversight done by different people than those involved in the authorisation process. This melding of the oversight and authorisation functions with the judicial commissioner is something that worries us. Down the line, looking at the Investigatory Powers Tribunal itself, I have spent nearly two years now litigating in this tribunal alongside some very well-known QCs from my old chambers and elsewhere who are well-versed in SIAC and other places where there are secret processes and unusual court systems. This court and these processes are the most frustrating and obfuscating that I have ever encountered in the UK system. We are talking about situations where, whether for intent or not—I am sure not, because everyone wishes this to be open—the bias is towards secrecy and not letting the claimant in to what is ultimately a determination of their rights and freedoms. That needs to change. All we have here is an additional right of appeal. There has been no further look at the procedures of the IPT, which allowed the Government to argue this year that, even if the tribunal made a determination to favour individuals—that they said behind closed doors, "This person's rights have been violated"—they should not have to tell the claimant. They could lie and still say, "No determination in your favour". We had a whole hearing on that topic. In the end the tribunal rejected it, but there is that level of vagueness and secrecy in the tribunal's rules. That simply has no place in a rights-compliant oversight and authorisation system.

Lord Hart of Chilton: Do you think, then, that there should be a blanket exemption for legally privileged communications?

Rachel Logan: That is the basis in English law. This is not a question merely of human rights law, this is about the common law.

Lord Hart of Chilton: No, but in respect of this Act.

Rachel Logan: Yes, we do. All there is here is a provision for codes to be available. We have to look at the safety of the justice system, as well as rights and freedoms. This is the most sensitive and the most basic principle. If I cannot, as a lawyer, say to my client that what they are telling me is entirely confidential, how can I know that they will feel free and safe and able to give me full information? There is a significant chilling effect from the mere fact of interception of legally privileged communications that really needs to be taken into consideration.

Lord Hart of Chilton: You mentioned a moment ago the Investigatory Powers Tribunal. Do you think that the provisions there are satisfactory? Again, I rather gather that you do not and that you do not think that the Investigatory Powers Tribunal provides a satisfactory route for appeal and remedy.

Rachel Logan: Indeed. The judgment we received from the Investigatory Powers Tribunal on 22 June was not in fact the final judgment in that hearing. The judgment on 22 June said, "There has been no determination in favour of Amnesty International; that is, you have not been unlawfully intercepted. There has, however, been a determination in favour of the Legal Resource Centre in South Africa—a very well-respected NGO—and the Egyptian Initiative for Personal Rights". On 1 July, having had a period for corrections and clarifications to the draft judgment, none of which were put into effect by the Government, we received an email out of the blue from the Investigatory Powers Tribunal informing us that there had been a mistake and where the judgment said EIPR, it meant Amnesty International. That was following a hearing that supposedly was looking in the most detailed consideration at our rights and at particular communications that had been intercepted and whether that was lawful and proportionate. We asked, quite rightly, "How can this happen?", and asked for an open determination explaining how a mistake of this kind had been made. We received a very unsatisfactory response from the tribunal. Indeed, Parliamentary Questions have been asked about this by quite a few Members of the House—both Houses, in fact—seeking a Statement from the Secretary of State, asking whether other human rights organisations have been in the same position, and nothing has been forthcoming. That casts light on quite how problematic the IPT currently is. It needs to be sorted out.

When it comes to the Investigatory Powers Commissioner, we set out in our written submission that it is mostly things around the edges, around independence and effectiveness. We would like to see the oversight and authorisation functions separated. This is a small group of people and they will be looking at the full process to see if it has been gone through appropriately, and reviewing that. In our view, it would be safer to separate out the functions of overseeing the process and undertaking the process, even if it is just a part of it.

Q204 Matt Warman: I would like to ask a supplementary question. Were you saying that there would be a chilling effect if legally privileged communications were intercepted? As I understand it, that power has already been avowed and therefore theoretically it is already happening and lawyers and their clients might reasonably worry about it. Has there been a chilling effect, given that this is something that could theoretically happen already?

Rachel Logan: I cannot speak for the entirety of the legal profession, I am afraid, I am simply one representative of it—and from Amnesty, obviously. It has certainly caused enormous

concern to us in how we deal with our clients. Amnesty does worldwide research and litigation on a range of human rights issues, often right at the edge of the issues that Governments are uncomfortable with; for example, looking at the involvement of our own Government in rendition and abuses during the war on terror. But we are also very much concerned with Governments overseas. It is very difficult for someone intercepting our material under a broad warrant to distinguish between what might be country research material and what might be professionally privileged because it concerns witness statements, instruction, et cetera. We are very concerned about the impact of knowing that material which is legally and professionally privileged is being picked up in their net.

Matt Warman: So has it had a chilling effect on your own communications?

Rachel Logan: I am not quite sure what you mean by that. Are we extremely concerned and worried about what we say? Yes, we are.

Matt Warman: Has that changed since the power was avowed in this country?

Rachel Logan: There is always a difference between when you worry that something is happening and when you are told that it actually is happening so, to that extent, yes.

Matt Warman: Moving on to communications services providers, from an NSPCC perspective, are you worried that communications service providers co-operate sufficiently at the moment, when information could help the kind of work that you do?

Alan Wardle: Generally, things are pretty good. Looking at issues particularly of child abuse images and how those are disseminated across the internet, Google and Microsoft—at the instigation of the Prime Minister—did some really good work a couple of years ago which means that it is much more difficult to find those images through an open search on the web. Now, with some 100,000 search terms, you get only what are called clean searches; that is, they do not give those images. So that has been good. Most of the big companies are involved with the Internet Watch Foundation. Certainly in this country we are pretty proactive so if an image is found, it is generally down within two hours, so that is pretty good.

On the content, because the majority of the big companies are American, you would have to ask the police. I am not sure how the investigation of the content of communications is working. We have an issue with some of the internet hosting companies, such as online storage functions where people are uploading and storing a whole host of images. We think that that issue needs to be looked at in more detail and we are looking at it at the moment. Most of the companies recognise that this is a very serious issue and they are generally very co-operative. It is a global issue so, while the UK is very seized of this issue, we are seeing some alarming developments in other parts of the world—such as livestreaming of child abuse, which is crowdfunded—which is why these sorts of powers are essential.

Matt Warman: Will the Bill improve that situation or not make that much of a difference?

Alan Wardle: Internet connection records are very important, as I have already indicated. When it comes to the information that is needed, the current process is often very convoluted, when you have to go through the MLAT process. Anything that could be done

to simplify and expedite that would be good. We know from the police that they do not even bother to apply for evidence in some cases because they know it will take too long.

Rachel Griffin: We have had feedback from police officers we have worked with on the National Stalking Helpline that communications service providers are not always helpful in cases where the police need their assistance. But we do not really know whether this unhelpfulness is to do with reluctance to help, misunderstanding of what help is needed, or because the legislation needs to change. What is clear is that CSPs, as well as improving co-operation with law enforcement agencies, need to provide more assistance to the victims, who are often seeking help, advice and protection after being targeted when using their services. Again, it is very difficult to say whether the proposals in the draft Bill will improve that co-operation without having a better understanding of what the barriers are perceived to be by the CSPs themselves.

Q205 **Suella Fernandes:** I have a follow-up question for Amnesty. You talked a lot about privacy rights. Obviously, we have to strike the right balance but I heard very little about national security. We have heard a lot of evidence and we have on the public record that the head of MI5 has said that we face an "unprecedented scale and character" of terror threat at the moment. We have heard from witnesses about very serious crimes that are being perpetrated online. You obviously do not feel that the draft Bill is satisfactory but where do you think the balance should be struck in meeting this very important need to safeguard the public?

Rachel Logan: There is of course a critically important need to safeguard the public. That is part of human rights protection and we all have the right to life and security and all those sorts of things. That is part of what we are looking for as an organisation. But as you say, it is a question of proportionality and where you draw the line. For example, I am sure that it would be useful for crime prevention and national security purposes if we all had to go round with a body camera on, videoing where we were at all times, and had to hand that tape over at the end of the day, or if we had to keep a list of everywhere we went and everyone we spoke to, and handed that over. That might well assist in preventing more crimes, but for most people that would be an intolerable level of intrusion into their private lives. For us, the Bill simply does not draw that line in the right place. Targeted, suspicion-based surveillance is a very different world from what is being proposed here.

Suella Fernandes: When it is necessary and proportionate.

Rachel Logan: This is the question. "Necessary and proportionate" usually means the least intrusive measure that can be used to achieve a legitimate aim. That is precisely the question that we are all here to debate and we do not think that the Bill has that line in the right place.

Suella Fernandes: My question to you, Rachel and Alan, is this. The Anderson review described Tor as a facility that enabled the digital abuse of anonymous activism and dissident activity. What is your view of this Bill's potential effect on encrypted communications in the context of your work?

Rachel Griffin: I would certainly refer you to those with greater expertise than me on the digital side of things, but my observation about encryption is that stalkers and cyberstalkers

are fixated individuals who will use any means available to them. We have had a number of cases where victims of cyberstalking have had their devices hacked by stalkers, and in those cases we have advised them to use encrypted services in future. We have experience of encryption being used for both good and bad reasons. Obviously a balance needs to be found, but I do not have the expertise in encryption to answer that question in an informed way.

Alan Wardle: Tor is a place where quite a lot of the most dedicated—if you can call them that—people who perpetrate these crimes go, particularly in the production and dissemination of child abuse images. Essentially it is a challenge for law enforcement. Being able to identify the perpetrators is very time-consuming, and I do not think that anything in the Bill will necessarily affect that. It is one of those things, given the way the internet is designed. A third of internet users across the world are children, but the internet was never designed as a child-friendly place, and we are almost going around saying, "Can you put safeguards in at the beginning?" Would you design it in this way now? I do not necessarily know that we would, but we are where we are, and certainly from our perspective the key thing, as well as power, is law enforcement dedicating the necessary resourcing and skills to get officers to do the quite painstaking work of cracking these rings of people, which are global and are perpetrating some of the vilest crimes against children. We need to ask encryption experts about that, but it is certainly challenging for law enforcement and we need to make that it has the resources—the powers, the skills, the expertise—to be able to deal with these policing challenges in the 21st century.

Suella Fernandes: I have one last question on a point that both of you raised earlier. You mentioned suicidal children getting in touch with you as well as tracking and trying to pinpoint people who are involved in stalking. Can you give us an idea of the need for timeliness in securing warrants in those situations? When you are in the process of an investigation or trying to track someone down, do you operate in a series of days and months, or is it hours and minutes that you and the law enforcement services need in order to exercise your powers?

Alan Wardle: For ChildLine it is hours and minutes. Someone will be called at 4 o'clock in the morning to breach that child's confidentiality, if that is required. There are cases of the police literally cutting down children who are found hanging and saving their lives. I was in a meeting with one of my directors not so long ago. They had to authorise something; the police intervened to protect a child who was about to jump off Tower Bridge. In those cases, it is a matter of hours and minutes, which is why there is a need for the systems that we have in place in CEOP, which are very fast and rapid. If a ChildLine counsellor and their supervisor think that the child is in immediate danger, sometimes that speed is of the essence.

Rachel Griffin: This is an excellent question, because it really helps me to draw out the distinction, as I see it, between our perspective and an organisation that is working on child exploitation. Very rarely will we deal with a victim of stalking where there is not enough risk information for the police to put protection around that victim based on a fairly well-established stalking risk assessment protocol. It is very rare—I cannot think of an example—that the information to put that protection around that victim was dependent on accessing communications data. The communications data concerns on the part of the

victims we deal with come about when evidence is being gathered to support an investigation and prosecution retrospectively. Given where stalking tends to sit in the list of priorities in a number of police forces, particularly digital stalking, which is perceived as difficult to investigate, that is where victims of stalking will end up, I fear—often at the bottom of the list of priorities.

Q206 Lord Butler of Brockwell: My final question is to Ms Logan, if I may, following up Ms Fernandes's question. Is Amnesty International opposed to bulk interference per se?

Rachel Logan: It depends on how you think about that question. Do we think that bulk interception draws the right line in the sand? Do we think it is a proportionate way of dealing with the threat? No, we do not.

Lord Butler of Brockwell: So as things are, you do not agree with bulk interception at all.

Rachel Logan: As currently laid out in the Bill, we do not consider that bulk interception—indiscriminate, suspicionless surveillance—is proportionate interference into an individual's rights.

Lord Butler of Brockwell: What needs to be done to the Bill to make it acceptable to you?

Rachel Logan: I am afraid that I can only talk to the parts of the Bill that we have assessed so far. We would like to see the provisions on bulk interception warrants stripped out. We would also like to see a change to the section dealing with so-called targeted warrants, which provides for incredibly broad thematic warrants, changed and provided with much tighter definitions. We would like to see a return to suspicion-based interference, the suspicion-based surveillance of individuals who are properly identified and properly targeted, as we would do normally in normal, day-to-day real-world life.

The Chairman: Thank you, all three of you, very much indeed. It has been a fascinating session. Thanks for coming along, and happy Christmas to you.

David Anderson QC (QQ 61-75)

Evidence heard in public Questions 61-75

Oral Evidence

Taken before the Joint Committee

on Wednesday 2 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Stuart C McDonald MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Bishop of Chester, Lord Hart of Chilton, Lord Henley, Lord Strasburger.

Witness: **David Anderson QC**, Independent Reviewer of Terrorism Legislation, gave evidence.

Q61 The Chairman: Welcome to you both. We very much look forward to what you have to say to us on what is obviously a very important Bill. I was going to ask a question that could be rolled into one, in a sense, if you have a statement that you would like to make. The question I was going to ask is: what do you think of the Bill? Perhaps you could answer that question and make any introductory comments to the Committee that you might like. You are most welcome.

David Anderson: I welcome this Bill, Lord Chairman. The law in this area has, until now, provided for extensive but vague powers, used in a way that the citizen could not predict and safeguarded by people who, for all their very considerable merits, have not been particularly visible to Parliament or the public. I would single out two major improvements that have already been happening over the 18 months since I started doing my review, *A Question of Trust*, though there is no causal relationship there, of course.

The first is the disclosure of significant and sometimes controversial powers that are already used but that people did not really know about before. You are looking there at bulk collection, the use of bulk personal datasets, the practice of equipment interference or hacking by the Government, and very recently, indeed on the morning the Bill was launched, a very significant data retention power that was previously almost entirely unknown. Many of those disclosures were prompted by proceedings in the Investigatory Powers Tribunal.

The second change is more proactive and visible oversight, in particular by the Interception Commissioner's office, which I single out because it is the office most concerned with the subject matter of the Bill, but also because it operates so transparently. This Bill, as it seems to me, cements those improvements and builds on them. I believe that there is now a complete avowal of significant capabilities, at least in outline. If I am wrong about that somebody was concealing them from me, and, although that is always possible, I do not believe that is the case. What I applaud about the Bill is that, for the first time, Parliament will have the opportunity, as it should in a democracy, to debate the capabilities that are used or that it is desired to use and decide whether it considers them acceptable or not.

The Chairman: Thank you very much. To both of you, I express the Committee's thanks for the reports you have produced recently, both of which will be immensely important for this Bill, but also for the public understanding of what you just described.

Professor Clarke: I convened a panel at the Royal United Services Institute, which we call the Independent Surveillance Review, consisting of 12 people who represented a pretty wide cross-section of interests, from ex-security chiefs through to people representing civil liberties arguments, practitioners, industry and so on. It was a very well-balanced group, but it was very wide. I am glad to say that our report was unanimous. We struggled with a lot of the issues and tried to take a publicly orientated view. We tried to start with big principles and then go down to the legislation, rather than starting with the legislation, because we thought that would be the most useful thing to complement David Anderson's review and the review of the ISC.

Our review was generally favourably disposed to the present situation, but we felt, as other reviews had felt, that the legislation was not clear enough as it was. This legislation certainly helps to clear that. The oversight regime, we thought, was critical both in warrantry and in the oversight, and it was not that it was incapable of being amended with relatively small changes. The most important thing was that we felt there needed to be much greater public confidence in it; it was not that the public were not confident in it, but they did not know enough about it. We felt that an oversight regime and a warrantry regime that could command more public confidence, which is partly where we brought the element of judicial oversight into the warrantry, would be very important.

The aspect of this Bill that is different from the expectations we had is the scope of what it says about equipment interference and internet connection records. That is controversial but is allowable for within the principles that we articulated. The differences between the Bill and our recommendations are comparatively small. I would be happy to go through them later on, but they are comparatively small. The approach of the Bill is pretty consistent with the review that we arrived at.

Q62 **The Chairman:** Thank you very much. Before I ask Lord Butler to come in, I will take advantage of being in this seat by asking my other question, which was to come later but touches on what you just described. It is the issue of trust and confidence, which appears to be at the root of all this, but particularly the issue of whether the new system will also produce improved confidence and trust in the agencies and the law enforcement bodies. Is that likely to be the case?

Professor Clarke: It certainly could be the case, because there is generally high public trust in the work of the agencies. They are fairly popular. There is more ambiguity over the work of law enforcement. It is bigger, more complex and covers a wider range of things. There is a degree of cynicism over some of that. There is a degree of increasing cynicism over the role of the state in general to intervene or interfere in the communications of its citizens. It must be a clean and clear oversight regime, with clarity and lines of responsibility that the public can follow. We recommend specifically that whatever arrangement is made for the commissioners should be very outward-facing, should try to publish more material and enter into a dialogue with the interested public that is wider than the dialogue that has been evident until now. That could be a big element in increasing confidence, not so much in the agencies, which do not need it, but in the police and in the role of Government itself.

On a final point, we began from the principle that this is not a series of technical issues. This represents something pretty fundamental in the bargain that the public make with the Government. In the digital age, this is the tip of a big democratic iceberg, and we have an opportunity now to get it right in a way that will be pretty important to the future of the political bargains we strike. This is one really important bargain that needs to be struck very explicitly and cleanly, as far as we can.

David Anderson: It struck me during my review that the people who need and deserve to be able to trust the system—not just the public, although public trust is very important—and who spoke to me most strongly about human rights, safeguards and the need to be trusted were the service providers, the telecoms companies that give assistance to Governments but are very nervous about being perceived to assist with things that are below board, and the intelligence agencies.

I had a message from somebody at GCHQ, which is probably too secret to disclose, but I will say it anyway because it is fairly innocuous. The reaction I had was, "I hope these new commissioners really make us work hard to prove that what we are doing is necessary and proportionate". If you are trying to recruit people on the pavements of Shoreditch to come and use their technical skills to work for GCHQ, you do not want to be seen to be working in some shadowy grey area where you are dodging in and out of the law; you want to be able to assure them that there is an absolutely copper-bottomed system in place. It is something that everybody wants.

People who are sceptical will be sceptical about safeguards as well. That is the way that people are. Commissioners will be portrayed, initially, as grey-haired old people out of touch. Judges will be portrayed as rubber stamps. That is why it is so important that what they do is transparent and they publicise their work, so far as possible. I would like to see judicial commissioners, for example, not just making wise decisions but issuing guidance, so far as possible public guidance, so that people can see how carefully they are thinking about it. I could go on.

The Chairman: It is hugely important.

Q63 **Lord Butler of Brockwell:** I would like to talk about the drafting of the Bill, if I may. Your two reports made recommendations in strikingly similar words. Mr Anderson's report said that the new law should be drafted in a way that is both "comprehensive and comprehensible", and the RUSI report said that "a new, comprehensive and clearer legal framework is required". Are you satisfied that the way the Bill is drafted sets out the powers and capabilities in as accessible and foreseeable a way as you had hoped?

Professor Clarke: Yes, from my personal point of view. I thought the explanatory notes that came with the Bill were pretty good, but the Bill itself is necessarily difficult because it combines a series of other legislative frameworks, which are very complex. We thought that one of the key elements of this sense of clarity would rest in the codes of practice. We said very specifically that the codes of practice should be written clearly in ways that ordinary people could understand. The Bill cannot be written in those ways, because it is a piece of statute legislation, but the codes of practice should be clearly written for the more general public. That, to us, would be a very important element of this whole package.

David Anderson: We set parliamentary counsel a probably impossible task, because we asked for a Bill that was comprehensive, and we asked for a Bill that was technology-neutral. It is quite difficult to be technology-neutral and at the same time explain exactly what it is that people are being authorised to do. I entirely agree with Professor Clarke that the code of practice, and not just that but other disclosure, is necessary.

If you are looking at accessible and foreseeable, it seems to me that it is not just about the Bill; it is about getting more material into the public domain as to the utility of some of these powers, in particular bulk, which sits there like an elephant in the room. We have heard discussions about how one can look to see if someone's wife is using the car and whether that is collateral intrusion and so on, but if you are tapping a cable that potentially gives you access to the conversations of thousands or hundreds of thousands of people, you are looking at some very major issues.

Nobody should expect the Government to give away operational secrets or information that is damaging to national security, but it seems to me that we need more in the way of information if this is to be truly accessible and foreseeable. A modest start was made by GCHQ; they allowed me to publish six case studies at Annex 9 to my report. I pressed them unsuccessfully to release more detail, and I was introduced to other case studies they were not prepared to publish. It was a very good start, and I hope more will come.

There are other grey areas that one would not know about from the Bill. This is not a criticism of the Bill, but, for example, can the intelligence agencies use related communications data, which is a by-product of bulk interception, to construct the web-browsing records of an individual? There have been some publications recently suggesting that they might be able to do that. One might think there is nothing particularly wrong with that, but it seems to me it is a relevant thing to know about, particularly if one is discussing internet connection records. If this new, highly regulated power should be introduced for the police to make use of, what about the agencies? Do they already have similar powers in this area?

As to retention, what exactly are the types of data for which the retention powers in Clause 71 could be used? There are all sorts of technical questions about that. One does not expect to see in the answer in the Bill, but Parliament will need to see some answers on those sorts of questions if it is to be able to debate this on a fully informed basis.

Q64 Lord Butler of Brockwell: If I may ask one supplementary question on comprehensiveness, there remains some other legislation with powers of intrusion, such as the Police Act and the Regulation of Investigatory Powers Act. They are not all being rolled into this Bill. God forbid that the Bill should be made even bigger, but do you think that is regrettable?

David Anderson: In a way, we have all stuck to our remit, and perhaps we were too obedient about that. The Intelligence and Security Committee, I do not need to tell you, was looking at the intelligence agencies. You said there should be a new law for the intelligence agencies and the rest could keep what they had. I was asked to look at interception and communications data, but I was not asked to look at intrusive surveillance, directed surveillance, all the stuff that happens later on in RIPA, so I did not make any

recommendations on that. I was not here for Sir Mark's talk, but I have heard him say in other contexts that he thinks that was a missed opportunity and it would have been nice to build some of those powers in as well. One could have built in all the Intelligence Services Act powers.

I suspect there are limits to what human beings can do in a short timescale. I do not often publicly praise the Home Office, whose work I review, but I must say they have worked extremely hard on this. There are people in the Home Office who I know for a fact did not get a summer holiday this year because they were working on this Bill. If one had expected them to do something twice as long, that might have been too ambitious.

Professor Clarke: The ISC, although it dealt only with the agencies, talked about reviewing the whole raft of legislation. We thought that would make the Bill impossible, and certainly impossible to get through in time to meet the requirements of the sunset clause. We stuck to the areas of RIPA and DRIPA and some of the other legislation that we thought was capable of being brought under a single legislative framework.

Mr David Hanson: You have touched on it there. We are talking about the legal framework, but I am interested, before we move on to the legal framework, about the assessment of either of you as to the deliverability of the 12-month holding of records, with both the provider and the Home Office being able to access those records. I wondered whether or not you had a view on that, as well as the legal framework.

Professor Clarke: My own view is that the Home Office, the agencies and the police can certainly have those powers, but they cannot exercise them entirely because of the international nature of the companies they are dealing with. One aspect of these proposals is that they will make it easier for companies who claim that they fall between different jurisdictions to comply with requests that they get from UK authorities, but they will not guarantee it by any stretch of the imagination. This legal framework will help, but in general the power of UK agencies to access as much as they have in the past is declining in any case.

Mr David Hanson: There is also the question of the funding. In the Bill, as we have already touched on, a large sum of money is allocated for support to the providers to deliver the service that the Government are expecting you or subsequent officials to regulate. Have you any assessment of whether those figures are realistic? We will return to that, as a Committee, in due course.

Professor Clarke: We have not made any assessment of that. The Bill came out after we finished our work, so I do not have anything to offer on those particular figures.

David Anderson: You asked about the deliverability of internet connection records. The first thing I would say about that is that the Bill has been a lot less ambitious, as it seems to me, than the old Communications Data Bill 2012, which I know some of the Committee knows very well. In particular, easily the most extensive and expensive feature of that Bill would have been the obligation on UK network providers to retain copies of all third-party data running over their networks. I think the very modest estimate for that was £1.8 billion, but it was accepted that it would probably be a lot more.

There is an estimate of about a tenth of that cost over 10 years for internet connection records. They have done what I recommended and made out an operational case as to the respects in which the police would find that useful. Does that mean they are deliverable? Not necessarily. I am not seeking to express a view on this, because I do not have one and I am not competent to have one, but there are some serious questions there. Another Committee, I know, is taking evidence on some of these questions. Would it be technically feasible to assemble precisely the types of data that they say are wanted? Would it be operationally worthwhile?

My understanding is that, although no other western country currently seeks to deliver internet connection records, there was an attempt to do something very similar in Denmark. This happened until June 2014, when the law was repealed. One of the stated reasons for that is that the police had not found it as useful as they had hoped. No doubt one can learn from other people's errors, and indeed I have heard that, in Denmark, they are thinking of reviving the idea. But it demonstrates that one cannot just run into these things without a deep technical understanding of how easy it is going to be to isolate and store precisely the types of data that the Government say they need.

Q65 Matt Warman: Going back briefly, I wonder if you could characterise to what extent the Bill, as it is, is a grand but not comprehensive tidying up exercise, versus the introduction of new powers.

David Anderson: For me, the headlines would be, first, transparency, as I said in my opening statement. It is key for democracy that the powers are out there. The second is enhanced safeguards at the authorisation level where intercept is concerned, and not so advanced when you are looking at communications data, and that would be one reservation I have. Thirdly, on powers, it preserves and makes explicit all the powers that are currently used and seeks to introduce one new one, the generation and retention of internet connection records by service providers.

Matt Warman: That makes it sound like you think the bulk of it is an aggregation exercise, with a small number of new powers.

David Anderson: Yes. It is a much more modest exercise in terms of new powers than the Communications Data Bill 2012. The reason it is so much bigger is because they bring into the Bill all these things that nobody had even heard of two or three years ago, but which are now set out.

Q66 Lord Strasburger: One of the powers you have already mentioned is bulk acquisition, which was only avowed on the day the Bill was published. You will be aware that the equivalent of that in the United States is Section 215 of the USA Patriot Act. You will also probably be aware that President Obama commissioned two reviews, in the wake of the Snowden revelations, and they both found that Section 215 powers were ineffective and do not make "any significant contribution to counterterrorism". It was duly repealed, with effect a few days ago, I believe. My question is: would this Bill take the UK into stronger and more intrusive powers when the United States has started to travel in the opposite direction?

David Anderson: It is dangerous and difficult to make international comparisons, although I am not discouraging it, partly because—and this is not a comment on the United States—

it is difficult to know exactly what is going on in other countries. I cannot put my hand on my heart and say that I understand the relationship between the Government and the former national telecoms provider in every European country or in the United States. I certainly would not have had any idea five years ago that the NSA had probes in the nine chief US internet companies, as was reported, under the PRISM programme.

There is, as you say, a parallel between a Section 215 power, where communications data internal to the US was gathered in one place, and the power that was avowed early in November, when the Bill was introduced to Parliament. We have seen the suspension of that Section 215 power. I think I am right in saying, although I might be out of date, that there had been rulings to the effect that the power is untenable because it was not sufficiently authorised by Congress. I do not believe that power has been tested against the constitutional guarantees of privacy, so I am not sure that one is necessarily saying that the American courts have gone further in relation to privacy, and indeed there are some respects in which they have not.

Lord Strasburger: Is it possible to answer my question in terms of avowed powers? Would it be true to say that avowed powers in the States are moving in a different direction to the one we are asked to move in with this Bill?

David Anderson: It is difficult to say, even in the United States. They have an executive order, 12333, pursuant to which all sorts of data are collected. It has not yet been reviewed. There is, I think, a proposal to review it, but very little is known about it. I could not tell you what the parameters of that power are, or what exactly it is used to do. You can give the Americans credit for a great deal, certainly in terms of judicial authorisation of intelligence warrants. They lead the world with the FISA court, and there are very few other countries that have attempted anything like that.

In terms of how useful 215 was, I hope that the utility and the proportionality of the newly avowed power will be tested before Parliament. I hope there will be a way of doing that. It may have to be done before the Intelligence and Security Committee. Of course, we already had a power, which everybody has known about for years, under the old data retention directive and now under DRIPA, whereby this sort of data can be retained by service providers. There may be a question as to the added value of retaining possibly similar categories of data in a single place. Is that all about speed of access, or are there other advantages that the intelligence agencies glean from it? It is a very intrusive power, and, if it is going to be justified, it is right that Parliament or Committees of Parliament should be given the opportunity to test its utility.

Professor Clarke: We spent in our panel, given the make-up of the panel, quite a long time thinking about bulk access as a matter of principle. Views differed across the panel. We all eventually came to the conclusion that it was necessary for the purposes of national security and law enforcement, and for all manner of intelligence purposes.

One of the problems in talking about bulk access in this context is that there is a sense out there that only Governments do it, but of course everybody does it. It is part of our digital society. The old phrase is that unless you are one of a very small group of people indeed, Tesco already knows a great deal more about you than MI5 ever will. Data analytics are used by everybody: by retailers, by charities like my own. Everybody uses data analytics.

Bulk exploitation of data is part of our society. When the Government do it, of course they should be held to a much higher standard because of what can follow from their conclusions, but bulk data is a fact of life. Our discussion is not whether we have or do not have it; it is how it is used and under what framework and what circumstances.

Q67 Suella Fernandes: In relation to bulk data, could you briefly give an example of how its possession has helped in intelligence and counterterrorism? I know there are many.

David Anderson: I can do it briefly by referring you to Annex 9 of my report. I only wish I could put names to the terrorists referred to in Annex 9, but I am told that I cannot. A few journalists have guessed, but that is as far as I can take it.

Suella Fernandes: The concern is that individuals who do not fall into the category of criminals or terrorists will have their browsing habits under surveillance and captured under bulk data, so my penchant for very expensive shoes and online shopping will be captured. Can you just describe the interest and the capacity among our law enforcement, intelligence and security services for that kind of information?

Professor Clarke: The safeguards in those cases rely on necessity, proportionality and legality, and the warrant that will now be required for bulk access will be much more specific. It comes down to the ethics of the agencies and the police, and how they operate the powers that they have. We on our panel were very impressed at the high ethical standards in general that apply.

The other great safeguard is the sheer physical capacity. One will be astonished at how little they can do, because it takes so much human energy to go down one track. The idea that the state somehow has a huge control centre where it is watching what we do is a complete fantasy. The state and GCHQ have astonishingly good abilities, but it is as if they can shine a rather narrow beam into many areas of cyberspace and absorb what is revealed in that little, narrow beam. If they shine it there, they cannot shine it elsewhere. The human limitation on how many cases they can look at at once is probably the biggest safeguard.

Lord Strasburger: You mentioned codes of practice. Governments have a habit of holding back codes of practice until long after Parliament has considered the legislation. Would you advise the Committee to urge the Government to publish draft codes of practice so that Parliament can see them while it is considering the Bill?

Professor Clarke: I would strongly advise that. That was a very clear conclusion from our work.

David Anderson: That is right. Of course, many of these codes of practice exist already. For example, an equipment interference code of practice was issued in February. You might notice, when you read it, it does not say much about bulk equipment interference, which is one of the aspects in respect of which some interesting questions are going to have to be asked. I would agree with that.

Q68 Lord Hart of Chilton: We have been asking witnesses about the judicial review principles that underpin judicial authorisation, and whether or not they constitute a true double lock system. Could you give us your comments on that?

David Anderson: I find it, as a rule, very foolish to disagree with David Pannick about judicial review. I think he knows more about it than anybody else in the world. I read his article and I agree with it, despite the fact it is not precisely what I recommended. It is much closer to what the RUSI panel recommended.

I would make one point in respect of which I think the double lock, in a sense, is unduly cumbersome. There may have been an echo of that from a previous witness. It is in relation to police warrants, which, in nearly all countries I know about, are perfectly straightforward: the police go to a judge and the judge gives them the warrant. It is not seen as an area where the intervention of a government Minister is necessary. I can see that, in national security matters, different criteria apply. Indeed, I recommended a double lock myself in relation to foreign policy and defence warrants. But in relation to police warrants, which are 70% of the whole and therefore represent 70% of those 2,300 warrants that the Home Secretary authorises every year, it seems to me that one could do without the politician or the Minister and go straight to the judicial commissioner.

Professor Clarke: We thought that the double lock, as the Bill came through, in principle is workable. It is undoubtedly more cumbersome than the present system, but that is probably a reasonable compromise in terms of bringing greater public confidence into the process and aligning us more with our international partners, which will have other advantages in persuading internet service providers to co-operate with requests they could argue they do not need to co-operate with.

Q69 **Bishop of Chester:** I was struck by Professor Clarke's expression: a "clean and clear" process of judicial oversight. Bishops, of course, are appointed in some sense by the Prime Minister, so I have to tread carefully here, but I am glad it does not have to be renewed every three years in my case. I wonder whether it feels right to have three-yearly renewal and the Prime Minister making the appointment, if you want to have a clean and clear process. I would be grateful for your comments.

Professor Clarke: This is a very powerful position and it will require the evident exercise of very high integrity that is unimpeachable. It is not difficult to find people who will do that, but they have to enjoy the confidence of the Prime Minister and the political establishment, and command public confidence as well. When I say "clean and clear", we had in mind the National Audit Office, a big organisation that has important technicians and specialists in it, but also has a big effect at the policy stages and in post-legislative scrutiny. Something approaching that is not unreasonable. The present system has been fairly ad hoc. It works reasonably well, but it could work in a much better way. It would be expensive.

We thought of four-yearly renewals, renewable for a four-year term, but three-yearly is not a bad compromise. I personally would prefer it to be longer, so that somebody could build a greater profile in the work that they do, which the public would get used to.

Bishop of Chester: Five years?

Professor Clarke: Yes, that would be workable as well. One of the important aspects of this role is the outward-facing nature of it. That is not an afterthought. It is important that the work of the commissioner should be outward-facing, seen and understood, in the same

way as Her Majesty's Inspectorate of Prisons. It is a really important role and the public should understand what that person does.

David Anderson: I see the advantages of a five-year term, and I see the advantages of making it a single term so that there would be no question of people being careful around the renewal period. I should say that I am appointed as Independent Reviewer of Terrorism Legislation for a renewable three-year term. Did that affect the timing of any fights I might have wanted to pick with the Home Secretary? I do not know; perhaps subconsciously it did.

Another thing to bear in mind is that it depends slightly who you want to do this top panjandrum job. It has to be a senior judge or a retired judge. If you want a serving judge—I am not suggesting that retired judges are not fully vigorous and capable of working six-day weeks, but that is the sort of person you probably want—and if you want to take someone out of regular judging for a few years and then put them back in the system, you might be pushing it to try to go beyond three years. They are familiar with the idea of the Law Commission: you leave the judiciary for three years to do the Law Commission and then you go back. If you are away from it for much longer, you might find people thinking, "Well, that is not really why I became a judge".

Bishop of Chester: And the Prime Minister making the appointment?

David Anderson: I ought to oppose that, I feel, because I understand the argument that it might be perceived as political, but I cannot help echoing what the judges have said to you. These are people who have been independent all their lives. They have been self-employed. They then took a judicial oath to show neither fear nor favour, and they do not. Yes, one could introduce consultation with the Lord Chief Justice, or by agreement with the Lord Chief Justice, perhaps bringing in the Judicial Appointments Commission and possibly some sort of parliamentary hearing. For the purposes of public perception, that may be a good idea. I suspect you would be better judges of that than I would.

Q70 **Stuart C McDonald:** First of all, I have a supplementary on a couple of things you said earlier. You both referred to a degree of public scepticism and cynicism, which largely arises because we are aware of all sorts of capabilities and practices being used that we had never heard about. How do these provisions prevent that from happening again? How can we ensure that things are not going on that we should know about but do not?

Professor Clarke: Partly because this Bill will tighten up a lot of powers and they will all be in one place. One of the reasons for some cynicism among those who took an interest in this is that they thought, as there were so many different legislative frameworks that the agencies or the police could use, it was almost as if there were loopholes that would allow them to do what they wanted. That was part of the basis of the cynicism. That would not exist to anything like the same degree under this legislation, so the tidying up and the clarity with which it could be presented, with the oversight, would provide a much greater reassurance.

As David said earlier on, those who will not be convinced will not be convinced by it. In a way, the battleground in terms of public confidence is the more average person, who feels that at least they know there is a process. They may not know the details of it, but they did

not even know there was a process until last year. At least if they know there is a process, they can take some interest in it and feel confident that the people operating that process are operating it independently.

David Anderson: In recent months, it has been the Investigatory Powers Tribunal that has been the main battering ram in securing avowal of programmes. That may conceivably be something of a one-off. I regret to say this, because I do not condone what Mr Snowden did, but it was information allegedly disclosed by Snowden that prompted some of those cases and eventually prompted avowal by the Government. I do not think that is a good model on which to proceed for the future.

The key has to be the commissioners. I have very high regard for what the commissioners have done, but I remarked in my report that it was not the courts, commissions or committees of London that disclosed to the British people what was going on; it was the revelations that originally came from Mr Snowden. That is not the way it should be. I hope one advantage of this big new commission, with the technical expertise, with the weight to get inside the agencies and work out what is going on there, is that these things will not come as surprises, and, if these commissioners feel there is something important going on that ought to be disclosed, they will write to the Prime Minister, as I wrote to the Prime Minister about the power that was disclosed on the morning of the Bill. I suspect they will find, as I found, that there is no resistance whatsoever to doing what is clearly right.

Q71 Stuart C McDonald: That is helpful, thank you. You have suggested that international comparisons might not be all that helpful. Nevertheless, I was planning to ask you about international comparisons, so I will do so. Are there ways in which this Bill, perhaps in its provisions relating to oversight, data retention, bulk collection, goes further than what similar countries have put in their legislation?

David Anderson: If one were taking a very general look at it, this is a very extensive set of powers, certainly by western standards. We are a major SIGINT power. That is reflected in the powers and that is why we need such strong safeguards to go with them. Moving away from those glamorous agency-type powers, one is also looking at things like the retention of quite basic call data by service providers, largely for the use of the police and other users of data.

Possibly reflecting the public mood in this country, although there are safeguards, they are not as tight as they are in some countries. For example, in Germany they have just reintroduced their own data-retention law. They require the data to be kept for four weeks, whereas the idea here is it would be held for 12 months. The Germans are going to require judicial authorisation for anybody who wants to look at it, which people are saying over there is going to be very cumbersome. Jo Cavan told you that there were half a million applications to look at communications data last year. Plainly, one could not ask people to go before a judge on each of those occasions.

As a nation, we seem to be less concerned about our own privacy, at least vis-à-vis the Government, than some of our neighbours in Europe and indeed across the Atlantic. That is probably reflected in what is a pretty strong suite of powers. That is why we need a strong suite of safeguards to go with them.

Professor Clarke: The only thing I would add is that there is an idea around this legislation that our country that has a high reputation in intelligence matters. We have a global intelligence capacity that not many other countries have, and that plays to our advantage most of the time. This represents a modern piece of legislation and, if the oversight capacity and the confidence that can be built into it are there, and if we put enough resources into it, it can be a world leader in legislative provision. One of the aspirations behind this thinking is that it would act as a very good example of how to get the balance right for a power that wants to retain high intelligence capabilities.

Q72 Stuart C McDonald: I have one final question. Correct me if I am wrong, Mr Anderson, but I think you said earlier that you some reservation about provisions relating to communications data. Could you expand a little on that?

David Anderson: One of the submissions I heard from a lot of people is that you can tell more and more these days from communications data. It is not any longer just the writing on the envelope; it can be the location data showing where someone was. Quite a lot of personal information can be detected, particularly when bulk personal datasets are combined. My reaction to that was not to say you have to bring in a judge every time. You cannot require a judge to authorise a simple reverse lookup when you are looking for a lost child in an emergency. But I said that there are categories of communications data requests that ought to be independently authorised, so why not by the commissioners?

I gave some examples—people looking for sensitive information about whom a lawyer might have been talking to and other novel or contentious cases, which is a concept that the commissioners would have to build up over time—that, it seemed to me, ought to be authorised by the commissioners. The commissioners ought to be able to put out guidance so that people would know the principles on which they were acting and you would have a principled framework governing these things, instead of the opinions of lots of different designated persons in different places.

Behind that idea was the way the law seems to be moving in Europe. There was a case, Digital Rights Ireland, last April, saying that you needed a prior independent authorisation even for quite simple communications data requests. The High Court this year decided that DRIPA was invalid because of a failure to give effect to that requirement. The Court of Appeal retrieved the position, from the Government's point of view, a couple of weeks ago by indicating that it was going to ask the European Court of Justice what it really meant. It will probably be 18 months or so before we find out the answer.

There is quite a lot of pressure from a number of angles. There were not many disappointments, to be honest, and I think they gave effect to the great majority of my recommendations and those of RUSI, but one reservation is that they did not do much to improve the authorisation of communications data, not just by police but by others as well.

Lord Butler of Brockwell: To follow up on that, how confident can you be that this Bill is going to pass the requirements of European law?

David Anderson: It is a very sensitive question, because the Court of Appeal has decided it is going to ask the questions of the European Court. I do not believe the questions have yet been finalised or sent off. If one restricts oneself to what has happened in other countries,

my understanding is that around five constitutional courts and some other courts, in countries such as the Netherlands, Belgium, Slovenia and Austria, have already decided that national laws based on the data retention directive, as ours was, are not valid. The High Court here said the same thing. The Swedes were made of sterner stuff; they asked Luxembourg the question, and so did our Court of Appeal. Trying to predict the results of litigation is a mug's game and I am not going to succumb to the temptation.

Q73 Matt Warman: You both implicitly mentioned the idea that this is the UK leading the world on the kind of legislation that we are going for in this area. The other side of that argument is that, if it is taken by regimes that do not share our judicial oversight and our values, it could essentially be misused. Is it ever reasonable to draft our legislation in the light of what another country might do with it for good or evil?

Professor Clarke: I would say no, because our legislation is for us. In a way, this will provide a model of legislation, because of the oversight provisions and independence that is meant to be built into that. If other countries that did not share the same democratic values imitated this but in a way that was a façade, that would be fairly clear.

One thing that we say in the RUSI report is that a start can be made by bringing together countries in the OECD and some of the like-minded liberal democracies. We need to create a much bigger consensus on the way in which legislation should handle this increasingly complex relationship between citizens and government in the digital age. This legislation could provide a basis for discussions with a lot of our partners. There will, of course, be quite big differences, because there are big cultural differences between the way Germany, the United States and Britain, let alone France, see these issues. There is a case for saying that a piece of model legislation would be a good example, and we should not try to second-guess what less democratic countries would do in response to it.

David Anderson: We are not at the privacy-minded end of that spectrum, but it is very important that we reach out and make our law understandable to people who are in a slightly different place. That is because this law has a huge extraterritorial reach. We assert the power to do a lot of things beyond our own frontiers. It is also because, as Professor Clarke was saying, to the extent that our law enforcement and intelligence agencies are seeing the world going dark, that is, in part at least, because there are internet service providers in other parts of the world, particularly the United States, that are wary of accommodating foreign Governments in their requests for information, particularly if those Governments do not respect what they see as the safeguards available in the United States, one of which is judicial authorisation.

I do not put it on the basis that we should set a good example for the rest of the world, although it would be an admirable thing if we could. I put it on the basis of self-interest, producing a law that is acceptable to the rest of the world, whether you are looking at courts in Luxembourg or tech companies in California, because that is the way to advance our own interests and to make sure that the people who need it can get the information they need.

Q74 Matt Warman: Finally, one of the crucial extra powers is the retention of internet connection records. Do you feel that that case has been adequately made publicly? Do you feel that the public have got behind that yet?

David Anderson: The Government have produced a 24-page operational case, as I recommended they should. I did not recommend 24 pages, but they have produced an operational case. They made out their case for three reasons why the police and others might want that information. That is now free for committees to interrogate, and no doubt you have started that process already. As I said earlier, the question marks that still remain in my mind relate to feasibility, cost, security of storage and all these other matters.

One always imagines the police will ask for all the powers they possibly can, but they are very conscious, particularly at a time of financial stringency, that they have to train people to use these new powers. They need to devote budgets to doing do. If it turns out to be a bit of a damp squib, as may have been the case in Denmark, they will feel they have wasted their money, so it needs a cool, hard look. I applaud the Government for doing that in relation to third-party data retention, which was said to be essential back in 2012 and which is now not essential anymore because it does not feature anywhere in the Bill. That has saved the country a very great deal of money.

I am not saying that internet connection records are in the same basket. I can certainly see how useful they could be, particularly in IP resolution and in tracing the fact that people have been using communication sites. How easy is that going to be to achieve technically, when nobody else in the world yet really does it? I do not know.

Professor Clarke: There is a principle behind that, which we talked about quite a lot in our panel. Is it the case that, in principle, law enforcement should have a right to try to go wherever the criminals are, or are there some areas in which we say, even if criminals inhabit them, the Government do not have a right to go? There is no easy resolution to that issue, other than to take a view, either yes or no. That, in a sense, is what we are talking about. Whether the adequacy of internet connection records as an investigative tool is correct, we do not know. We just do not know how useful it will be, but it does raise exactly that principle. Do the Government have a right to go anywhere where the criminals might be?

Q75 **The Chairman:** I have one final question, which relates to the first one I asked. You are satisfied with the draft Bill, by which I understand that you are satisfied that the major recommendations of both your reports have been taken on board.

David Anderson: I have not totted them up. I can say that around 90% or more of mine have been wholly or substantially taken on board. Although my report, I am afraid, is very long, most of it is descriptive and the recommendations themselves fit into about 20 or 25 pages, whereas this Bill is closer to 200. For me, the challenge is going down a level into the detail and seeing whether those who have applied themselves to that detail have made all the right decisions.

Professor Clarke: As Chair of the RUSI panel, I can say that the Bill met most of our expectations in terms of the recommendations that we made. Also, at the end of our report, we elucidated 10 principles and said any future legislation must meet those 10 tests. I would recommend you have a look at those tests. I think the legislation meets most of them.

The Chairman: It has been a fascinating session. Thank you both very much for coming along. I am sure you will be interested in the recommendations we eventually give the Government. Thank you very much indeed.

Professor Ross Anderson, Professor of Security Engineering, University of Cambridge (QQ 76-93)

Evidence heard in public Questions 76-93

Oral Evidence

Taken before the Joint Committee

on Monday 7 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Bishop of Chester, Lord Henley, Lord Strasburger.

Witness: **Professor Ross Anderson**, Professor of Security Engineering, University of Cambridge, gave evidence.

Q76 The Chairman: We extend a very warm welcome to our four guests this afternoon. We are very grateful to all of you for coming along on what is a hugely significant Bill that is going through Parliament—the Prime Minister called it the most important of this Session. Thank you very much indeed. As you probably know, the procedure is that I will kick off with a question or two, and then my colleagues will in turn ask you various questions on different aspects of the Bill that I think you find very interesting. If, when I ask a question of an individual, he wants to preface his remarks with a short statement, that is entirely up to him. I turn first to Dr Bernal. After you have answered, colleagues will be able to come in. What are your views on the draft Bill? Does it deliver the transparency on investigatory powers that you have particularly called for?

Dr Paul Bernal: Perhaps the best way to put it is that it goes part of the way. As far as I am concerned, it is good to see everything in one place, or almost everything—some bits are clearly missing—but for proper transparency we do not need just the Bill; we need the process to work properly as well. I would have said in my introductory remarks, had I made any, that the timetable makes it very difficult to get as much scrutiny as we would like; we have been called here very rapidly, and you have only a few weeks to do this. For transparency to work properly we have to have the chance and time to put our analysis into action. It is a bit difficult to do that.

One other thing I would say about transparency is that certain terms are used and expressed in a way that is not as clear as it could be. There are terms like "bulk powers" when we do not really know how bulky "bulk" is, if you see what I mean. For things like Internet connection records, it has taken some time, and we are still only part of the way there, to tease out what it really means. From that perspective, it is good to have it all in one place, but the process needs to be stronger. We need to make sure there is enough time to do it, and I am not sure you have as much of it in this Committee as you would like—perhaps later on there will be time—and we have to tease out some of the terms more accurately.

There is one other aspect. Some of the things in the Bill will become dependent on codes of practice and similar things that go with it. For transparency's sake, so that we understand what is going on, those codes of practice need to be put in a form that we can all see prior to the final passage of the Bill.

Q77 The Chairman: You have touched on the second question I was going to ask, so I will raise it now. You mentioned the codes of practice, which are hugely important in all this. What do you think the legal status of those codes might be?

Dr Paul Bernal: The legal status of the codes depends a little on how the final Bill turns out. From our perspective as legal academics, the key thing about codes of practice is not so much their legal status, which, depending on how it is set out, will be clear, but the extent to which they are also subject to the level of scrutiny and attention that the Bill itself is. It is easier to pass a code of practice through a small statutory instrument than to pass a whole Bill with full-scale scrutiny. We want to make sure that the codes of practice, which can be the critical part, get the same degree of scrutiny and attention both from people like us and from people like you.

The Chairman: With regard to the timetable, of course the issue that affects both this Committee and Parliament is, as you know, the sunset clause in the current legislation. Parliament has now laid down the amount of time we have. We certainly ensured that we gave ourselves extra and longer sessions, including in and around Christmas, and I am quite convinced that both Houses of Parliament will give it very thorough investigation, as indeed they should, but the point has been made. Does anybody else wish to speak on those issues?

Professor Sir David Omand: If I may make two remarks, the first is to stress the importance, in my opinion, of the Bill as the culmination of 500 years of history. It has taken 500 years to put the secret surveillance activities of the state under the rule of law. For centuries we had the royal prerogative being used in secret. Parliament passed the device of the secret vote but asked no questions. We had executive regulation in the last century, and for the past couple of decades we have had a patchwork of provisions in legislation, so all that secret activity was lawful but not understood. This Bill now places it under the rule of law; it will be comprehensible to the citizen. I cannot overestimate the importance of the Bill.

The second point is to agree strongly that it is in the codes of practice that the public will find it easiest to understand what is going on, rather than in the technicality of the Bill itself, so the codes are very important. Schedule 6 to the Bill sets out very clearly what the status of those codes will be. They will have to be presented to Parliament, along with the enabling statutory instrument.

The Chairman: Professor Anderson or Professor Ryan, are there any comments you would like to make at this stage before we move to other questions?

Professor Ross Anderson: I believe you will be asking me in due course about Internet connection records.

The Chairman: We will.

Professor Ross Anderson: It would be great if, in addition to having codes of practice, we had very much greater clarity on definitions. I will discuss Internet connection records, but there are other things that are not really defined at all, from the great concept of national security down to some rather technical things. I hope that clarification comes out during the Bill's passage.

The Chairman: You think such definitions should be on the face of the Bill.

Professor Ross Anderson: Yes.

The Chairman: Professor Ryan, are there any initial comments you would like to make to the Committee?

Professor Mark Ryan: Just on questions 1 and 2?

The Chairman: At this stage, yes, because there will be other more detailed questions, some of which will probably be directed to you personally as well, but at the beginning of the session would you like to make any general comments?

Professor Mark Ryan: The comment I would like to make about transparency is that this seems to be such an important area that the kind of oversight proposed is not enough. One would need more quantification of the sort of surveillance that takes place. Of course, I am aware that surveillance has to be done in secret, but I believe that the quantities of surveillance and the nature of surveillance can be disclosed to people without compromising the secrets of the surveillance activity. That seems to go more towards transparency and is much stronger than mere oversight, so I believe there should be more of that.

Q78 **Dr Andrew Murrison:** You have covered a huge amount of ground in about seven minutes. You hit the nail on the head in terms of definitions and the need to ensure that codes of practice and statutory instruments are sufficiently transparent and that scrutiny is of the utmost. I am interested to know how you think scrutiny and transparency can be improved other than through the normal process of laying statutory instruments before the House, because I sense from what you said that you feel that the Bill, which talks about SIs and codes of practice, is not sufficient in that respect.

Dr Paul Bernal: I would not say exactly that it is not sufficient. What I am interested in is getting as much scrutiny as we can. In order that we can understand the Bill we need to have the codes of practice at the same time, at least in draft form, so that they can be examined; frankly, to understand some of the powers in the Bill without a code of practice is very difficult, particularly on things like bulk powers and Internet connection records. We will talk a lot about Internet connection records later, but they are defined in such a way that it is unclear on the face of the Bill exactly what they will mean in practice.

Historically, not as much attention is paid to statutory instruments by the House. You do not spend as much time passing them as you do Bills; you do not have Committees scrutinising each of the statutory instruments at the same level of detail.

Dr Andrew Murrison: But it is worse than that, is it not? This is a very rapidly moving field, so you cannot reasonably lay all the codes of practice and anticipate all the SIs at this time, since 12 months down the line there may be yet more to come.

Dr Paul Bernal: Yes, and that is a fundamental problem with any kind of Bill in this area. I do not know whether there would be a mechanism to produce better scrutiny of the codes of practice, but attention should be drawn to the fact that this will be important as it continues. It needs constant attention, not just at the moment we pass the Bill.

The problem with the Regulation of Investigatory Powers Act was that, although it got a lot of attention at the time, the things that gradually built up to create the confusion—chaos is not quite fair—for people about the overall regime, and which stimulated the need for this Bill, were not sufficiently attended to over the years as things happened. We need to make sure that does not happen this time around.

Dr Andrew Murrison: Do you think a sunset clause would help? We are replacing one sunset clause with another. Is that inevitably where we are going to be led?

Dr Paul Bernal: Frankly, in this area you need sunset clauses in almost everything, because the technology moves and the behaviour of people changes. The overall situation changes. You need to be able to review these things on a regular basis, and a sunset clause is one of the best ways to ensure that happens.

Professor Ross Anderson: Last time around how we dealt with this was that, in the run-up to the passage of the Regulation of Investigatory Powers Bill through Parliament, a number of NGOs organised a series of conferences called Scrambling for Safety, and afterwards various statutory instruments were laid before the House. We are proposing to do the same again. The first Scrambling for Safety workshop is to be held at King's College London on 7 January from 1 pm to 5 pm, and all members are of course very cordially invited. We anticipate that it will be the first of a series that will enable engineers, lawyers, policymakers and others to dig into the meat of what is going on, exchange views and push the thing forward.

Q79 Suella Fernandes: Based on your expertise, would you set out briefly the nature and extent of the problem or threat we are facing when it comes to the use of this technology?

Professor Ross Anderson: The problem with the use of surveillance technology is that, if it is used in ways that do not have public support, it undermines the relationship of trust between citizens and the police, which has been the basis of policing in Britain for many years. Sudden revelations like Snowden are extraordinarily damaging because they show that the Government have been up to no good. Even though the Government may come up with complicated arguments about why bulk equipment interference was all right under Section 5 of ISA and so on, it is not the way to do things. There was a hearing in the Investigatory Powers Tribunal last week on that very issue.

There are other issues. The first is national leadership. If we go down the same route as China, Russia, Kazakhstan and Turkmenistan, rather than the route countries such as America and Germany have gone down, there is a risk that waverers, such as Brazil and India, will be tempted to follow in our wake. That could lead to a fragmented IInternet, with

extraordinarily severe damage for jobs, prosperity, international stability and, ultimately, the capability of GCHQ to do its mission, because if you end up with the IInternet being partitioned into a number of walled gardens, like the Chinese or Iranian ones, they will be very much less accessible to the intelligence agencies.

In addition, if the powers are abused, or seen as capable of being abused, there could be exceptionally serious damage to British industry. If people overseas come to the conclusion that, if they buy a security product from a British firm, it may have a GCHQ-mandated back door, they will not buy it; they will buy from a German firm instead. This is where the rubber hits the road when it comes to overreach in demanding surveillance powers.

Professor Sir David Omand: On the other hand, my advice to the Committee would be that this Bill contains the basis of the gold standard for Europe. This is how you get both security and privacy in respect of freedom of speech. The interplay of checks and balances and oversight regimes means that none of what Professor Anderson has described needs to happen. Of course, with a malign Government and agencies that flouted the law it would be possible to have abuses. I do not believe that either is likely, and certainly the provisions in the Bill allow this House to maintain very strict control of the Executive in its use of these powers.

Professor Ross Anderson: With the greatest respect, the reaction of America and Britain to the Snowden revelations has been somewhat different. In America people have rowed back in all branches of government. For example, President Obama has, simply by executive order, commanded the NSA to minimise the personal information of unaffected foreign nationals, like us. The legal branch has seen to it that, for example, national security letters, which used to be secret for ever, are now disclosed after three years, and Congress failed to renew provisions for the retention of American citizens' communications data. All branches of government have pushed back and sent a solid signal to the world that America cares about privacy and the proper regulation of its law enforcement and intelligence services. If the reaction from Britain is different, even if powers are not abused, it still sends a signal to the Brazils, Indias and, may I say it, the Kazakhstans. We do not really want that.

Q80 **Bishop of Chester:** A sunset clause is the nuclear option of legislation, but reading the Bill I am wondering how there is a process of inbuilt review, because the scene is changing so fast. There is a technical supervisory board bringing together stakeholders and so forth. Should there be an inbuilt power to renew the provision? That has been in some previous terrorist legislation. There has not been a formal sunset clause, but there has been a renewal motion. That would force Parliament to review what is happening, because for the legislation to continue there would have to be a renewal notice.

Professor Sir David Omand: Of course, it is Parliament's prerogative to put in such a provision. My experience in the public sector is that it should be done very sparingly, because it may turn out that at precisely the moment you have to legislate afresh, as with DRIPA, Parliament may not actually want to legislate afresh. One concern I had was whether the definitions in the Bill were sufficiently robust to deal with technical change. Having studied them, I am as confident as I can be that they avoid hostages to fortune, so your House will not discover in a couple of years' time that a different Bill is needed because the technology has moved on, but that will need to be examined by detailed scrutiny.

Q81 Shabana Mahmood: My first question is to Professor Anderson and then his colleagues. We have two competing narratives of the Bill: one that these are significant new powers and major changes, and the other that it is just codifying current provisions and bringing them more obviously and explicitly within the rule of law, as Sir David suggested. Professor Anderson, what is your view as to which of those narratives is more accurate?

Professor Ross Anderson: The Bill has been marketed as bringing in only one new power, namely Internet connection records, but it does many other things as well. For example, when the Regulation of Investigatory Powers Bill passed through this House and became an Act, one of the things we lobbied for and secured was the provision that if the agencies wished to command somebody to decrypt something, or hand over a cryptographic key, there should be special safeguards. The City of London did not want a rogue superintendent, perhaps in the pay of a criminal gang, to approach a 24 year-old assistant shift supervisor at a bank's data centre somewhere in east London and command him to hand over the bank's master signing key. Therefore, the provision was made that the production of a cryptographic key had to be demanded by a Chief Constable in writing and the letter had to be presented to a main board director of the bank. There are many provisions like that which appear to be swept away by this new legislation. Parliament must realise that the arguments are just as strong today as they were then; otherwise, how are you going to persuade international banks that London is a good place to do business? Some banks already had issues last time around.

My second comment is that a number of things that were previously done secretly were made public only in the run-up to this Bill, which enables the Bill team to say, "This is old stuff. We knew about it already". I refer members to the Investigatory Powers Tribunal hearing and the long arguments therein about whether an ISA Section 5 warrant could be used for bulk interception or only targeted interception. There are many technical aspects like that.

Thirdly, although the Internet connection record is ostensibly the new thing in the Bill, it actually gives very much greater powers than have been advertised; rather than just helping IP address resolution, it enables a policeman to say, for example, "We have these two bad people. Show us all the websites they both visited last month, and tell us the names and addresses of everybody else in the world who visited the same addresses". That is an extraordinarily powerful capability. It is the sort of thing that Internet service companies use to fight spammers, phishermen, click fraudsters and so on. Those of us who have worked in that field know how powerful it is and tend to be of the view that it should be classified along with intercept. If we are to have a special higher burden for intercept warrants, that higher burden should apply also to complex queries that are made on traffic data.

Shabana Mahmood: Have you done any analysis of powers advertised one way but which, as you suggest, lead to, say, five extra things? Have you made some sort of qualitative analysis to back up the examples you are helpfully giving us?

Professor Ross Anderson: The qualitative analysis basically comes from experience working at Google on sabbatical four years ago with the click fraud team. Knowing that such inquiries are extremely powerful, and talking to colleagues at Yahoo and Facebook recently, there is general concern that, if you allow people to make complex queries like that, it is up

at the level of a box of fancy tricks; it is not the sort of stuff you want to let an ordinary policeman do without supervision, because it can be used to do some very bad things.

Professor Sir David Omand: The Bill does not provide for ordinary policemen just to request that. There is a mechanism for a single point of contact and independent agreement before data can be acquired. I do not recognise either of the extreme cases Professor Anderson puts forward, but no doubt the Committee will need to investigate that further.

Dr Paul Bernal: If I may add something in response to that, there is something missing in the idea that these are either new powers or old powers. People's behaviour has changed fundamentally. The Internet, which was a medium used for communications—in the old-style idea of communications—is now used for almost everything else: shopping, dating, research and that kind of thing. The same power applied in a different situation gives a significantly higher level of intrusion than we have ever seen before. It is not like listening to phone calls, reading emails or things like that; it is like following people down the street while they shop, looking at the books they take out of the library and things like that. Without even changing the law, you are significantly changing and increasing the level of intrusion. It has lots of different implications, not just in terms of the balance of privacy and things like that but all the other rights we normally think of. Our expectations of privacy are different from those we had in the past. In a way, it comes down to the idea of how the law is going to change and how we need to take things into account. We need to take into account not only developments in technology but the way people's behaviour changes in relation to that technology; for me, in effect, that is the biggest increase in power. It is not that there is a new power built into the Bill, but because we use communications so much more extensively it is a much more intrusive thing to do any kind of Internet surveillance.

Professor Sir David Omand: That is why the Bill defines event data, Clause 193, in a conservative way, not taking modern metadata but imposing on the rather fuzzy reality some precise definitions, to minimise—it cannot be avoided completely—the kind of case Dr Bernal referred to. Inevitably, if you impose strict definitions on fuzzy reality, you will occasionally get hard cases. Those will exist in this world. As we know, the difference between dangerous driving and driving without due care and attention means that sometimes cases fall on the wrong side of the line, but the old adage that you do not make law by hard cases still applies. I commend to the Committee the way that the Bill has not expanded the definitions of communication data in defining event data.

Q82 **Shabana Mahmood:** That is helpful. You touched briefly in your previous answers on my final question, which is about future-proofing the Bill to take account of the pace of behavioural and technological change. We had evidence from officials from the OSCT. They were very bullish and confident that the changes in relation to Internet connection records in particular meant that it was sufficiently future-proofed. Could we have your comments on that?

Professor Ross Anderson: I have two main comments. The first is from the viewpoint of the long term—20 years out. We are simply asking the wrong question. The right question is: what does the police service look like in a modern technological society? Is it completely centralised? Does it go like Google? Do Ministers take the view that a chap sitting in Cheltenham can learn more about citizens in Leicester than a bobby on the beat in

Leicester? What sort of society does that become? This is a much broader conversation than just about who gets access to whose mobile phone location trace when.

The medium-term issue, which I think will become acute over a period of five to 10 years, is that the real problem is a diplomatic one. The real problem is about jurisdiction and how we get access to information in other countries, specifically America. America is where the world's data are kept. If they are kept in Finland or wherever because of cheap electricity, usually they are still controlled by a US company. There are some exceptions—Korea, Japan et cetera—but this is largely about how we get access to American data.

That means, like it or not—and many people are beginning to come to this conclusion—that the real fix for this is a cyber-evidence convention, like the cybercrime convention. That will involve diplomatic heavy lifting and an agreement, perhaps initially between America and the European Union, with other willing countries joining later as they wish, that provides a very much faster service for getting at stuff than the current mutual legal assistance treaties. For that to work, there are three things we almost certainly have to have. The first is warrants signed by judges, because that is what America expects. The second is transparency, which means that if somebody gets wiretapped you eventually tell them—when they get charged or after three years or whatever. The third is jurisdiction, because the real bugbear for companies like Google at the moment is that a family court in India gives it a warrant saying, "Please give us the Gmail of this person in Canada", who has never been to India. How do you simultaneously employ engineers in India and give privacy assurances to your users in Canada? That is why at present all this stuff gets referred to lawyers in Mountain View. That is the real problem, and it is time the Government faced up to it.

The Chairman: Professor Ryan, do you want to say something regarding an earlier point?

Professor Mark Ryan: I want to go back to the question of whether these are new powers or existing ones. Following what Dr Bernal said, one of the very huge powers that exists in the Bill is bulk equipment interference—that the state can interfere with people's computers on a bulk scale—which means that people who are not guilty of any crime, nor even suspected of any crime, may have malware put on their computers by intelligence services to collect vast amounts of data on innocent people in a kind of funnel, so that eventually criminals can be caught, but the people who are being subjected to that are not criminal at all. That seems to me to be an extremely dangerous thing in a free society. I do not think that the kind of oversight proposed in the Bill goes anywhere near being able to control that type of activity.

Professor Sir David Omand: The bulk equipment interference warrant can be sought only by the intelligence agencies in order to acquire intelligence relating to individuals outside the UK for the purpose of national security. For the sake of clarity, the Bill already restricts that.

Q83 Lord Strasburger: Sir David, your career was spent in senior positions in the Civil Service deep inside the security establishment, which probably makes you, of the panel, specially qualified to answer my question. It seems that over the past 15 years decisions were made behind closed doors to introduce several of the most intrusive and least overseen powers in this Bill without bothering to seek Parliament's approval. Why was it considered acceptable in

a democracy to bypass Parliament and introduce large-scale and highly controversial surveillance powers without Parliament's explicit approval?

Professor Sir David Omand: I can only hazard an answer, which is that the legal regime under which previous Governments operated for the past 20 years, since the 1980s, was what I would describe as legal compliance; in other words, if it could be done lawfully under existing powers that Parliament had passed, Ministers would authorise such activity, after due legal advice, regardless of party—this is not a party political matter—in the interests of national security, the prevention and detection of serious crime, and economic well-being arising from causes outside the United Kingdom. That was the regime.

It was really when the Investigatory Powers Tribunal took the case and reported that the Government's activity, in particular GCHQ, might be regarded as lawful under the individual statutes but failed the rule of law test because it was not clear, as your question implies, to the public—

Lord Strasburger: Or to Parliament.

Professor Sir David Omand: Or to Parliament. This Government have taken that to heart, and the Bill is in part the result. We have moved into a new era and I am personally very glad of that. A lot of trouble would have been saved if, say, even five years ago the codes of practice—it would not necessarily have taken new legislation—on equipment interference, investigative powers and so on had all been updated to the modern digital world. For one reason or another that was not done. The shock of discovering what was happening, for very good reason—to defend the public and our security—was all the greater. I think the lesson has been learnt.

Q84 **Victoria Atkins:** I have a question for Professor Anderson and Dr Bernal. You talked a lot about privacy and, in particular, the debate in America about privacy. One thing that strikes me about the whole discussion is that very often we are focusing, if I may say so, on the worst-case scenario as to what the intelligence services and the Government will do with people's information. What are your views in relation to the computer companies that hold all this data about us? If we google a dating agency, Google will have that information. What are your views on those bodies, because to me they are very much part of the debate about privacy?

Professor Ross Anderson: Yes. I tend to take different views of different companies because of their different internal cultures. Having worked at Google, I understand and to some extent trust the culture there.

Victoria Atkins: You worked at Google.

Professor Ross Anderson: Yes, four years ago on sabbatical, so I understand it. My colleagues have worked for other companies. Fundamentally, whether you are a company that tries to be good or a company that is a bit less scrupulous, the underlying fact is that the modern economy depends on people trusting large service companies with their data, because it is so much more efficient to have 100 million people's data in a data centre than it is for everybody to be backing up their own hard drive at home and losing their photos

and everything. That trust has to be maintained. If it is lost, the consequences could be dire for economic growth and the companies concerned.

People talk about worst-case privacy scenarios, but that is how people talk; that is how the media and politics operate—they operate by stories. The human brain is optimised for stories; it is how people remember stuff. If you get the perception out there that in the UK people who offer services have to leave a government back door, or remove the encryption if ordered, or whatever, it could be extraordinarily damaging for British business.

Victoria Atkins: Does selling people's data come into that? Are you comfortable with Google's position on that, having worked for it?

Professor Ross Anderson: Personally, I do not click on ads. If you want to go to a company that does not sell data, you can go to Apple or you can go to the trouble of having everything private. For example, I take the view that, if I am sending an email that I do not mind the FBI reading, I use Gmail; if I am sending an email that I do mind the FBI reading, I use something else. That is also the conclusion to which I think more and more users generally, and young people in particular, are coming to.

Q85 **Matt Warman:** I have a question for Dr Bernal primarily. As an example of new powers in this Bill, you said it was like following someone down the street and seeing which shops they go into. It strikes me that we have long had the power under certain circumstances for people to be placed under surveillance and followed down the street to see which shops they might go into. Could you give the Committee an example perhaps when we get back?

The Chairman: Order. There is a Division in the Commons, so we will adjourn for 10 minutes. I am sorry about that.

The Committee suspended for a Division in the House of Commons.

Matt Warman: To recap briefly, you cited the example of following a person down the digital street under authorised surveillance, which strikes me as a digital updating of analogue powers we have already. Could you offer the Committee an example that is not simply a digital updating of existing analogue powers and is genuinely novel because it is digital?

Dr Paul Bernal: It is a very important question, and there are lots of issues related to it. There are some things that we do in the real world, or the offline world, that we feel comfortable being observed doing. We have CCTV cameras in the streets, we have them in shops, and so on. We do not have them in our bedrooms, we do not have them staring at our diaries all the time and we do not have them monitoring exactly where we walk. We get the choice: do we want to go to this place where we know there is CCTV, or that place where we know there is not CCTV? That is one of the important differences.

The thing about the Internet as it is now, particularly for younger people, is that they do literally everything on it; there is no aspect of their lives that does not have an online element. If you have a system as is proposed with Internet connection records, for example, where there is some gathering of their entire browsing habit, not beyond a certain level—I hope we will get on to Internet connection records later—at least you have knowledge

about what they are doing in every aspect of their lives. When you go to the doctor, you expect confidentiality from your relationship with the doctor when you discuss your health issues. If you visit a website to research a particular health condition, that may reveal just as much about you as you would reveal to your doctor—in fact, many times more than you might reveal, because people have a sense that they can get more intimacy by doing things on the Internet than they might even be prepared to admit to a doctor.

There is another element. We talked a little about Google and others. Given the way profiling works for almost all commercial Internet companies, and the way big data analysis works, you can draw inferences from relatively small amounts of browsing data that can then be used to infer stuff that you would otherwise keep private. An example is your sexuality. You might not want to reveal your sexuality, but big data can make a probable analysis of it with a relatively small number of places you visit on the Internet.

It goes back to the question about whether we are looking at extreme cases. We are looking at extreme cases in some ways, but we are also looking at very ordinary cases. What we all do on the Internet has an impact on credit ratings, insurance premiums and things like that. They can be based on very basic information that can be gathered about how we behave.

I am sure David will say that safeguards are built into the Bill so that it can be used to do only certain things, but that is not really the whole story for two reasons. One is that data, wherever they are and in whatever form, are vulnerable in many different ways. The example that comes most readily to mind, because it is so recent, is TalkTalk having been hacked, and holding exactly the kinds of records that we are talking about. That information is ideal for ID theft, credit card fraud, scamming and things like that.

If we gather those Internet connection records, we are basically creating a very targeted database, which says on the front, "Hack me, please, if you want to get ideal information for these kinds of crimes". We need to be careful not just about what we think the Government are going to do. Like David, I trust to a great extent our security services and police, but we are creating something that can be misused by other people, not just by them. There are many ways in which that can happen.

Q86 Suella Fernandes: In terms of legality, the issuing of warrants is subject to the test of it being necessary and proportionate. In light of that, what is your view on its compatibility with proportionality as required under the ECHR?

Professor Sir David Omand: Proportionality and necessity are in the Bill. They are written in, as they are in the current legislation. Dr Bernal's examples were very good ones of why digital mass surveillance is a thoroughly bad idea. Thankfully, it does not happen now, and under the provisions of this Bill it could not happen in the future either. The question that I suggest the Committee really needs to address is how proportionality is assessed—precisely your question—not just in relation to the granting of a warrant but the whole process through which the selection of material for examination by human beings—the analysts—takes place. The IPT, the independent court, has examined this; senior judges who oversee interception have examined it, and they are satisfied that the current procedures are consistent with the Human Rights Act, Article 8 and thus respect privacy. Equally, there is no reason why the provisions cannot be applied in practice in ways that remain consistent.

The decision on proportionality and necessity rests with the person signing the warrant. The Home Secretary has made her view clear in the Bill. I am disappointed that she decided that she had to sign police warrants and that they would not go direct just to the senior judge for approval, which was our recommendation in the independent review commissioned by the former Deputy Prime Minister, and that would be more consistent with David Anderson's review. I strongly believe that the Home Secretary or the Foreign Secretary, as appropriate, should sign the warrants relating to national security and the work of the national intelligence agencies, for which they are statutorily responsible to this House. The police service is in a different constitutional position, and I would have thought that purely police matters could go straight to the judge. It is no harm that the Home Secretary signs as well; it is just additional work.

Dr Paul Bernal: Can I go back to the question of proportionality? One of the key things is not just about the warrant to access the information. One of the key elements of proportionality is the gathering and holding of the information itself. The CJEU has consistently—even more so recently—held that the holding and gathering of the data engages Article 8, and that indiscriminate generalised holding and gathering of data is contrary to fundamental rights. That was held in Digital Rights Ireland; in the Schrems case it was part of the key reason why the safe harbour decision was invalidated. This is not because they have some perverse view that does not match with reality but that the European Court has started to understand the impact of holding all this personal data. It is not just the warrants—to a degree, I agree with David about the warranting process; it is the gathering of the data that I disagree with, particularly the way Internet connection records are set out. All this data seems to me to be gathered on the assumption that that is all okay and it is just the accessing we need to deal with. I cannot see how this law would survive a challenge in the CJEU on that basis.

Professor Sir David Omand: I very strongly disagree. I am not a lawyer, but it seems very clear to me that the Schrems and the Digital Rights Ireland judgments do not bear on the point that has just been made. Those judgments did not consider the question of proportionality of collection and selection, which is not indiscriminate collection of data willy-nilly. You might want to take advice on that.

Professor Mark Ryan: I want to comment on the bulk provisions of the Bill, because they allow for the collection and automatic processing of data about people who are not suspected of any crime. Therefore, I do not think it is correct to say that this is not a recipe for mass surveillance. It is the processing of data about everybody, and in my opinion that is mass surveillance.

Professor Sir David Omand: But it is not processing data about everybody.

Q87 **Baroness Browning:** We have covered quite a bit of my question about definitions. Clearly, we have differing views on the panel. Sir David, in your evidence to the Science and Technology Committee I believe you suggested that somehow you would never get a perfect definition, and in the absence of that a pragmatic approach should be taken. Do you want to identify the balance between being safe and being practical?

Professor Sir David Omand: The starting point has to be the value of communication data both to the police and to the intelligence agencies. The police evidence is very clear. It has

huge importance in ordinary crime as well as in countering terrorism and cybercrime. From that starting point, we have to have an authorisation process that can cope with the number of requests, which is over 500,000 a year, so talking about requiring warrants to be signed by Secretaries of State or senior judges is not appropriate. The justification for that was that it is less intrusive to look at communication data than to look at content, and that principle is reflected in the Bill.

The point I was making to the Science and Technology Committee is that there will be some hard cases, and Professor Anderson gave some examples of precisely that. If you move the cursor too far over to be so restrictive, you create a real problem about the authorisation of data communication requests. If you move it too far the other way, you get the equal and opposite problem of not sufficient authority being applied. The cursor is more or less in the right position, because it has taken the RIPA 2000 definition of who called whom, where and what, and transferred it to the computerised age of which device contacted which server up to the first slash of the address, but there will be hard cases. I was suggesting to the Committee that you have to be pragmatic and ask whether the overall public interest in the authorities and police having this information, which is vital for upholding the law and bringing people to justice, balances the fact that you may occasionally have a hard case. In my view it certainly does.

Baroness Browning: If we get the definition right and if we get the clarity that the panel seems to feel is lacking at the moment, do you think that will serve us for now, or will we have to keep revisiting this?

Professor Sir David Omand: For the sake of clarity, I think the definitions are clear; it is reality that is fuzzy. The parliamentary draftsman has done a very good job trying to clarify this. I am not sure you can make it any clearer.

Baroness Browning: That is very clear. Thank you.

Dr Paul Bernal: This is a really important element. Sir David said that communications data was less intrusive than content. I do not think that is true. They are differently intrusive. There are several reasons communications data can be more intrusive. One is that it is by its very nature more suitable for analysis and aggregation. You can do more processes to it than you can to content. That means that it is subjected to what we loosely called big data analysis. It is also less hard to disguise in some ways. You can talk about a coded, not encrypted, message to somebody. In England we do this all the time; when we say “quite”, it could mean a million different things depending on the context. You cannot do that so easily with communications data. That means that sometimes you can get more information out of communications data than you can from content. I do not think you should be under any illusions that somehow it is okay to have as much communications data gathered as possible but not okay to get content. They are different things. For individuals, sometimes content matters more; en masse, communications data matters more.

The Chairman: Before you came in we were discussing the differences between communications data and content, but the drafters of the Bill and the Government who sponsored it seemed to indicate that there is a significant difference in terms of people’s

privacy with regard to what is written by them and to them, as opposed to the hows, the wheres and the whens, but you are contesting that.

Dr Paul Bernal: I am contesting that. I would say that it can be worse. You have at least some control over what you write, whereas for communications data largely you have very little control over it at all. It is a different sort of intrusion.

Q88 **Baroness Browning:** From the point of view of the speed at which things change, could you indicate whether you think that even if we had an imperfect definition, in your terms, we are going to have to keep coming back to legislation more quickly to update it? Is that a danger?

Dr Paul Bernal: Frankly, yes.

Baroness Browning: Do you think we will keep coming back to this?

Dr Paul Bernal: I think you will be coming back to this and you should be, because things change in so many different ways. This is not the sort of law that you can set down and say it will last for 15 or 20 years without amendment, because the technology is moving too fast; people's behaviour is changing too fast.

Baroness Browning: May I bring you back to Sir David's point? Seeking perfection is perhaps something that we should compromise with pragmatism.

Dr Paul Bernal: You should, but you should compromise it by adding extra oversight rather than by accepting a loose definition, by making sure you can monitor what the intelligence and security services and the police are doing so that pattern of behaviour matches the intent behind the law as well as the definition. This is part of Lord Strasburger's analysis of how powers have grown without parliamentary approval. It is very easy and we have seen it historically again and again. People have not been watching what is going on and you need to continue to monitor things. I am not yet convinced that the oversight arrangements here are strong enough to do that. The idea of, if not a sunset clause, a revisiting clause of some kind might be worthwhile, and also monitoring the monitors: how are the oversight arrangements working?

Q89 **Stuart C McDonald:** Turning to communication service providers and the requirement that could be placed on them to store up to 12 months' worth of communications data and Internet connection records, how feasible is it for providers to do that?

Professor Ross Anderson: It could be extraordinarily difficult and expensive if they are to do what they are advertised to do. We are told that Internet connection records will enable the agencies and police to get past what is called carrier-grade NAT, which is a technique whereby the IP address of your mobile phone might be shared with 1,000 other mobile phones, the idea being that, if someone does a bad thing online on Monday, you ask O2 and they say that it could be any one of 1,000 phone numbers, and, if the person does another bad thing on Wednesday, you have another list of 1,000 phone numbers and you say, "Aha! The common number on the two lists is this one". It is not going to work that well, first because you will find hundreds of common numbers on the list; and, secondly, if you want to relate that to things people have done on other service providers, you have to

relate it to an ID on Google, a handle on Twitter or a logon for Facebook. For that, you would have to require the communication service providers to store very much more data than they do at present. You would have to get them to store precise time stamps, addresses and so forth, which they will not do.

ICRs will not work as advertised. What they will do is create an extraordinary capability power for investigators to say, "Show us all the websites that these two bad people have visited in the past month and all the other people who have visited the same websites". If you want that capability, which appears to be what is intended, you end up requiring lots of people to store lots of stuff. There is, first, the issue of cost if you are to remunerate communication service providers in Britain; and, secondly, there is the likelihood that service providers overseas will refuse outright because it would be too much effort and energy to redevelop their systems, and Britain is only 4% of the market anyway.

Dr Paul Bernal: The Danes are the people who have got closest to doing this, and I would recommend, if you can, to get one of the witnesses from the Danish abandoned attempt. They ran it for nearly seven years and got almost no useful information out of it, but there was a huge cost, even though they were warned beforehand by the ISPs, as I believe they will be here, that this is not a practical proposition and is not likely to be an effective one.

Professor Sir David Omand: The Committee will discover, if they do that research—I hope they will—that the model the Danes chose is not the model I strongly suspect the Home Office would choose. The Danes themselves are revisiting it at this very minute because they may find post-Paris that it is necessary to go back and look at it.

Q90 **Matt Warman:** I want to talk a little about encryption or decryption. Do you think it is reasonable for Government even to ask communications providers to provide unencrypted material for something that is currently encrypted?

Professor Ross Anderson: There is a power in Section 3 of the RIP Act which allows them to do that. As I remarked earlier, Parliament saw fit to hedge it with very stringent safeguards. Nowadays, it would be much more difficult, because many service providers encrypt stuff by default. They do so not out of any particular malice towards agencies but simply to stop other people stealing their ads and customers. It has just become the commercial default; it is what everybody expects. With messaging services, everybody increasingly expects stuff to be encrypted end to end. The Government of Kazakhstan have recently decreed that everybody has to install the Kazakhstan Government's cert on their machine from 1 January. I predict that if you have an iPhone in Kazakhstan you will suddenly find that none of the services works. That will be worth watching.

Matt Warman: Sir David, do you have any thoughts on whether we are likely to get anything meaningful out of demanding unencrypted data from people who currently encrypt it anyway?

Professor Sir David Omand: Of course, you will be distinguishing between content data and communications data, which clearly has to be delivered in a form in which the authorities can use it. If we are looking at content data, as far as I can see there is no back-door encryption provision in the Bill. The Government have said that they are not seeking it. I know the agencies are not seeking it, so as end-to-end encryption spreads it will get harder

and harder for the authorities to be able to access unencrypted content, even for their highest priority suspects. That is a fact of life.

Does that mean that the authorities should have no power to seek such information, and to do their best in cases where it might be available? That is the approach I would commend to the Committee. It is a power to seek, but I do not think it is in Parliament's power to insist that all encryption can be bypassed, nor would it be a very sensible thing to ask for in terms of the national economy and the need for the Internet to be secure. There will be specific cases where it will make sense and information could be made available, and the Bill should provide for that.

Matt Warman: To be clear, in general you do not see the Bill as providing the back door that people have spoken about.

Professor Sir David Omand: No, I do not.

Dr Paul Bernal: Many of the companies concerned do not share Sir David's view, and that is one of the reasons why some of them are distinctly disturbed by news of the Bill. One other thing that we need to be very clear about—Professor Anderson has already referred to it—is that we do not want to put British companies at a disadvantage, because they are more likely to be subject to the force of British law than a company in California or Korea. If we put the power in place to allow them to do it, they are disadvantaged, and that is not good for anybody.

Matt Warman: Which only emphasises the need for clarity, does it not?

Dr Paul Bernal: Clarity is what is needed.

Q91 **Matt Warman:** To move on to equipment interference, what does the panel understand that to be?

Professor Ross Anderson: It is basically hacking or the installation of malware, or what the NSA calls implants and what we call remote administration tools in a machine. If I am a bad person, the police would be able to say to O2, "Put an update on the android on Professor Anderson's phone", and that would enable them remotely to turn it on, use it as a microphone or room bug, or look at me through the camera, collect my location history and all the rest of it. What is more, as we get digital stuff in more and more devices they could do the same to my granddaughter's Barbie doll; they could do the same to your car or your electricity meter. It is open season on the Internet of things. It goes without saying that the controls around that need to be very carefully drawn; otherwise, it undermines trust. If UK producers of stuff can have their arms twisted to provide a capability to put implants into stuff, why should people buy stuff from Britain?

Professor Sir David Omand: I agree with the point Professor Anderson makes about the need for careful oversight of this, but the power already exists; it is already in use under existing statutes, including the 1994 Act. It is of inestimable value to the intelligence agencies, particularly on national security addressed to targets overseas where there are

legitimate demands for intelligence. Some 20% of GCHQ's output benefits from that kind of technique. There is nothing very new about it.

Dr Paul Bernal: There is nothing new about it, but there is something new about our behaviour and the technology we all use. Twenty years ago I was not using anything that was encrypted at all; now half the stuff I have on my phone is encrypted by default, and another batch is encrypted by choice by me, so for normal people this now becomes relevant when it was not relevant before.

Professor Ross Anderson: What is new is that we found out about it thanks to Edward Snowden, and GCHQ admitted that it was doing it just in the last month or two, thanks to the case currently before the Investigatory Powers Tribunal. People are beginning to get worried about it, and with due cause.

Q92 **Lord Strasburger:** Gentlemen, can you help me out with bulk personal datasets? The Bill and the Explanatory Notes are very vague about that. The ISC report was rather vague about it—it was hugely redacted. The Home Office will not tell the Committee the identity of the databases it is scooping up, so it is very difficult for this Committee to assess the proportionality, risks and intrusiveness of the collection of bulk personal datasets. Does anybody know what they contain? Do they contain medical records? Do they contain bank records? What do they contain?

Professor Ross Anderson: For starters, we know that the police have access to things like credit reference and DVLA records. That is public knowledge. Secondly, they have access to medical stuff. They have had that since 1996. At the time, I happened to be advising the BMA on safety and privacy and that sort of thing came through. Thirdly, in any case, hospital medical records were sold on a wide scale in the care.data scandal last year, and it would have been rather negligent if GCHQ had not grabbed a copy on its way past. Fourthly, it is well known that some kinds of bank records, in particular all international financial transactions, are harvested on their way through the SWIFT system.

Professor Sir David Omand: Not true.

Professor Ross Anderson: This has been a matter of enormous contention in the EU and elsewhere. It is only to be expected. If I were, for example, an investigator for the FCA, I would want everybody's bank statements too.

Professor Sir David Omand: Chairman, it is important not to allow fantasy to intrude at this point. The central bank governors responsible for the SWIFT system agreed that that system could be searched for specific transactions of known criminals and terrorists. That is public knowledge. All SWIFT data is not scooped up.

Lord Strasburger: Perhaps we could impress on the Home Office the need for the identity of these databases to be revealed.

The Chairman: That is something that we would have to do in private session, but I take the point that there is a serious difference of view between the witnesses on what is a hugely important subject.

Q93 **Dr Andrew Murrison:** I am going to be fairly brief, because I think we have covered quite a lot of this already. I refer to the international dimension. We sit here thinking we can make various laws and regulations, but we are talking about a global industry. Referring to some of your previous comments, could you reiterate the likely reaction of the international community to the Bill, in particular the feasibility of gathering ICRs, given that it is entirely in the gift of companies whose headquarters are not in the UK?

Professor Sir David Omand: We took evidence on this as part of the independent surveillance and privacy review run by RUSI and we got a variety of answers from international and British companies. Some of the companies said that as a matter of corporate social responsibility they wanted to be in a position to provide this kind of information for the purpose of preventing serious crime and terrorism, but they felt extremely nervous about doing it without a firm legal basis on which warrants or authorisations would be made. Other companies said that as a matter of company policy they did not believe their data should be made available to any state or law enforcement authority. You have a variety of views. The provisions of the Bill, which include the provision that the Home Secretary can make judgments about what it is reasonable to expect, will be partially successful; but they will not be completely successful, because some companies will simply refuse, and I cannot see the British Government attempting to launch civil actions against major players.

Dr Andrew Murrison: Presumably that means that the disinclined would note those who were complying and those who were not and go for those who were not.

Professor Sir David Omand: The intention is not to make public the companies that comply and those that do not.

Professor Ross Anderson: We all know the companies that will comply. They are the ones that get large amounts of their revenue from Governments, or that rely on Governments for capture regulators—companies such as IBM, BT and those set up several generations ago. Companies that have been set up in the past 20 years think differently because they have a different culture—the Silicon Valley culture. Their money comes either from their users directly or from advertising—from their users buying stuff or being advertised to—and they take a completely different view. It is not much good getting BT on board if all BT is doing is providing a piece of copper wire from people's houses to where the real action starts, so it is the view of the big American service companies that matters more than most. They are going to drag their heels.

There is the issue of foreign Governments. There is also the issue of what happens to small start-ups in the UK, which is absolutely crucial. For example, about five years ago one of my postdocs set up a security start-up. Because of the arm-twisting that the agencies have always indulged in, he decided to set up a coding shop in Brno in the Czech Republic. More and more people will be doing that, simply as a matter of default. You cannot run a tech start-up nowadays unless you have a marketing operation in North America, because that is where you make your first sale and most of your initial sales. If we create a regulatory regime where it is only common sense for people to put their coding shop, their

engineering, in North America, Seoul, Mumbai or wherever, the cost to us directly or indirectly down the stream of time will be huge.

Dr Paul Bernal: We have to be aware of where things are moving. There may be a number that are co-operating willingly now, but that will shrink. More and more companies are likely to say, "No, we are not going to give this", and they will be the bigger and more successful ones. You make yourself a hostage to fortune by assuming that this will end up functioning.

The Chairman: Thank you very much indeed. I thought the whole session was absolutely riveting. You have given us an enormous amount to think about. Obviously, you have very different and varying views on the issues before us, but you highlighted issues that very much need highlighting. I know that members of the Committee are grateful to all four of you for giving us your very robust and significant views on this important Bill. If you would like to add any written evidence to supplement what you have said, we would be more than happy—indeed delighted—to receive it. Thank you very much indeed.

Adrian Kennard, Managing Director, Andrews & Arnold Ltd (QQ 116-126)

Evidence heard in public Questions 116-126

Oral Evidence

Taken before the Joint Committee

on Wednesday 9 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Lord Henley, Lord Strasburger.

Witness: **Adrian Kennard**, Managing Director, Andrews & Arnold Ltd, gave evidence.

Q116 The Chairman: Welcome and thank you for coming along to give evidence to us on a Bill which is extremely important for the country and for organisations and companies like yours. I am going to ask you a fairly straightforward question to begin with, but if in answering it you want to make a general statement, please feel free to do so. How extensively has the Home Office engaged with you with respect to the provisions contained in the Bill?

Adrian Kennard: Not at all really. As a small ISP, the only involvement we have had is that ISPA—the Internet Service Providers Association—was invited to a briefing after the Bill was published to try to explain it to us. That is the only involvement we have had.

James Blessing: As ISPA we tried to engage beforehand. We made representations. There was not a long dialogue until after the Bill was presented. It has been a bit difficult on that side of things. As a service provider—I do both—there has been no conversation whatsoever.

The Chairman: It is perhaps important to explain to the Committee that Mr Blessing acts in two capacities, with his own company but also as chair of ISPA.

Q117 Lord Butler of Brockwell: In the absence of discussions with the Home Office, to the extent that you have been able to think about what is proposed by way of separating communications data from content, have you any view about whether it is practicable?

James Blessing: It is practicable as in it can be done. It is not practicable in many senses because it is not clear what is required to be done. Because the Bill does not on the face of it say exactly what is required to happen—what information is required to be captured, what format it is to be stored in and how it is to be made available—it is very difficult to design a solution that works and does all the things it needs to do, which is secure, safe and retains the data needed by law enforcement to continue its investigations. Part of the issue is that the Internet connection records do not exist. They are not a thing. They are not generated in normal business. We do not have them. They are a new thing that has been created, and because they are not defined it is difficult to say how you would go about creating them.

Adrian Kennard: I have concerns about the definitions as well. The communications data depend hugely on the context of the communication. The definitions make something like a phone number communications data, but that should only make sense in the context of a telephone call. If it is buried inside an email, is it still communications data? It seems that the Bill could consider it that, and could give the Home Secretary power to have a snoop on the content of information to pull out anything that is an identifier, like an email address, a phone number or someone arranging a meeting. It is quite important that the definitions relate to the context of the individual communication.

Lord Butler of Brockwell: Where do you expect that definition to be made? Are you expecting it to be made in the code of practice—clearly there will be further work—and how long do you think it will take?

James Blessing: In an ideal world we would like it in the Bill itself. Having what is required clear and transparent in the Bill makes it easy for everyone to understand what is being collected. The Internet industry is slightly different from many other industries in the fact that we depend on each other to be able to do what we do. Therefore, we tend to discuss in open forums solutions to problems that we commonly have. If collecting Internet connection records became a thing and it was clearly defined—"This is what they are"—it would be something we would sit down in rooms and discuss and for which we could come up with solutions that worked for us. Our networks are all very different. They are all designed, grow organically over time, and change and adapt depending on the types of customers we have, so there is no single solution that will work for everybody. Even with two networks that look very similar, their solutions will not work, because they will have some exceptions that cause a problem. Unless that is clearly codified in the Bill itself, it makes trying to work out what is going to happen very difficult. The code of practice has not been published. Even a draft version of the code of practice has not been published, which again leads to the problem that there has been no scrutiny, no review of it. From my understanding, the Internet connection records are going to be defined in individual orders from the Home Secretary, which leads to another problem in that we cannot discuss them with each other. There may be operational reasons—we do not know—but the problem is that we have no visibility and no way of talking about them because we are prevented from discussing them with any other party.

Adrian Kennard: It is worth pointing out that the previous regulations provided a very specific, clear menu on the face of the regulation as to what could be retained—telephone numbers for telephone calls, text messages and email addresses. It would be massively helpful if the Bill spelt out exactly what data need to be recorded; what there is currently an operational justification for retaining should be spelt out in the Bill. That would help massively with these discussions, because we would be able to understand what we might be asked to record.

Lord Butler of Brockwell: Would it not be a little inflexible to put it in the Bill, because as technology changes and the world goes on, you would need amendments? Would it be sensible for it to be in a statutory instrument so that it is there in public and everybody can see it?

James Blessing: It would, as long as it is some form of document that is published so that we can all see it and discuss it. Statutory instruments would work as well, as long as they can be discussed in public.

Adrian Kennard: If that is to be the case, it is important that what the initial SI will be is available when the Bill is considered by Parliament, because what data needs to be recorded has a massive impact on costs. I know technology changes over time, but I am not sure that granting the Secretary of State such wide powers with those very vague terms is justified simply in the name of future-proofing. It does not usually work.

Lord Butler of Brockwell: Directions from the Home Secretary are unsatisfactory because they are confidential. Is that the point you are making?

Adrian Kennard: That is important.

James Blessing: It is important.

Q118 **Dr Andrew Murrison:** I do not have much more to ask on this particular bit, Chairman, except to say that the definitions are rather refined in this piece of legislation compared with its predecessor legislations, which in part this is meant to replace. I am getting from you that we have a long way to go yet for this to be in any way a workable document, and that you would prefer to see the codes of practice or statutory instruments published at pretty much the same time as the Bill, since without those the Bill is pretty pointless, is it not?

James Blessing: Yes.

Dr Andrew Murrison: Is that it, in a nutshell?

Adrian Kennard: Yes, I think so. You say they are more refined. The previous regulations were very clear—telephone numbers, email addresses. This is about identifiers that could refer to equipment somewhere in very vague terms.

Dr Andrew Murrison: Forgive me, I was thinking more about electronic data than about telecommunications—telephone—data, which I accept are much easier to record and are recordable in any event for billing purposes. This is in a different space entirely, is it not?

Adrian Kennard: Yes. I am sure ISPA and telecommunications operators would be happy to work on coming up with some clear definitions to help you, to specify in clear terms what an Internet protocol address is and what an email address is, to give you an idea of what those data are and how they could be written down.

Dr Andrew Murrison: I am slightly disappointed that the Home Office has not already done so, because we are presented with this whopping great draft Bill, yet we are pretty unclear about the definitions; indeed, when questioning your predecessors on the panel and asking them to put it on a Likert scale of zero to 10, where zero is rubbish and 10 is extremely good, they said it was zero, which is a cause for concern.

Adrian Kennard: That sounds a bit negative.

James Blessing: There are some nice bits in the Bill that clarify a few things in a nice way. They are a rare beast within the Bill as a whole.

Adrian Kennard: I get the impression that the Home Office has spoken to the larger ISPs. It said as much in the meeting we had. In order to come up with the cost estimates it must have a clear idea what information it is asking for. While we would love to help specify the data that can be collected so that that can be put in the Bill, the Home Office has just left it out. I do not think it is that it does not know. It must have an idea to get the costing.

Dr Andrew Murrison: It is simply relying on putting it in a supplementary piece of legislation.

James Blessing: Or not putting it in any legislation whatsoever and just doing it as part of the notice from the Home Office.

Adrian Kennard: I think that is what it wants to do.

Q119 Suella Fernandes: When it comes to the issuing of retention notices, you understand that there will be an assessment whereby the Home Office is not going to issue them on all service providers. It takes into account the costs, the feasibility and the volume, and that is going to be informed by the Technical Advisory Board. There is a heavy element of discretion and consideration as to the practical implications. You appreciate that, do you not?

James Blessing: We appreciate that very much and it is the correct approach. The problem is that operational needs change, and the requirement for an ISP suddenly to get a notice because its particular group of customers is of interest to law enforcement means that we all, as service providers, have vaguely to sketch out how we would do that. When it is a nebulous "We are not quite sure what we are doing", you can do that, but you cannot plan to say, "I will make these changes to my network should I get that notice". As part of the Bill, we have gone from a situation where cost recovery was quite clearly stated as, "It is definite that you will get your cost recovery", to a slightly woollier version, which says that the Home Office "may" provide some cost recovery.

Suella Fernandes: But it is clear there is the duty to consult. It is very much a two-way process.

James Blessing: Yes.

Suella Fernandes: Lastly, there is also a power for you to appeal, whereby if it is disproportionate, whether on a practical or cost basis, the decision can be reviewed.

James Blessing: Again, that is absolutely fine. It is built into the system. We appreciate that, but, as someone who runs an ISP, the problem is that I have continually to assess threats to my business and threats to the operation of my network; and, at the moment, the Home Office turning up and saying, "You are going to have to start retaining this data", is classed as a threat. It is not that it might destroy our business, but it is going to take a lot of focus from my projects to provide service in rural areas or deploying the network in London. It is going to stop me concentrating on doing that part of the day job. There is absolutely no method in the Bill for recovering any of those lost opportunity costs, so I have to put together a pot of resources on the side, just in case. If the Bill specified exactly what I had to do, I could probably get to the point where I could put it into a background level, have a

plan and know exactly what I am going to do and how I get from there to there; and, when the Home Office turned up with a retention notice, the actual process of getting from the request to its being enabled would be a lot shorter as well, which, from an operational point of view, is beneficial.

Adrian Kennard: The key thing is that we do not have certainty in our business because we have this potential hanging over us. It is worth pointing out that the definitions in this Bill are very vague on who can be subject to these notices. It could cover schools, coffee shops providing wi-fi and it could cover businesses. They are all providing communications, albeit not as a business and not to the public, so for any business with any sort of IT department there is suddenly potential huge uncertainty over them with this Bill. It would be a lot clearer if the Home Office identified the operational requirements it has at the moment, which it has said are large ISPs, and the Bill pinned that down and said it has to be large communications providers.

Q120 Mr David Hanson: You will have heard the question I asked other colleagues earlier, which is, effectively, what your understanding of an Internet connection record is.

Adrian Kennard: The Home Office tried to explain it to us. Essentially, it was whatever you are ordered to collect, with huge scope for what that could be. We had discussions this morning when we were talking about event data, which seem to be about an event that does not have to have a place but has to have a time and at least one person and involve a communications service. If I have a conversation on the phone with a friend and say, "I am going down to the pub tomorrow", that is not an event, but if I say, "I am going down to the pub because they have really good wi-fi", that could count as event data because it relates to a communications service. It is so vague that, no, we do not know what it is.

James Blessing: The Bill itself does not make it clear. It is part of the concern we have raised repeatedly that, because it is not in the Bill, the code of practice has not been published and there is nothing else there, it is very much—

Mr David Hanson: Given that it is within a certain scope—we all roughly know, because the definitions on page 25 are what the Government think it should be, even if it is not nailed down yet—how easy do you think it is to do? If we said to you today that the Bill had gone through both Houses of Parliament and there was an implementation date of six months after it had gone through both Houses of Parliament, could you do it?

James Blessing: If you said that every telecommunications provider—it would cover an awful lot of people you did not realise it covered—was to be mandated that it must be able to record Internet connection records, it would be expensive. My network is not set up or designed in any shape or form to record this information, because I have as a business no need to do it; therefore, I would spend a lot of money on hardware. Six months is doable, but the other side of the coin is getting the data to law enforcement when it requests it in a format that makes sense for it. That is probably more work than installing new hardware across my network. I am going to have to send engineers to Cornwall and Aberdeen, but that could be done. It is about the actual amount of other things where we collate all that information and then present it in a format that works.

Mr David Hanson: Adrian, you are a smaller provider. How does that impact on you?

Adrian Kennard: You said the definition is in the Bill.

Mr David Hanson: It is on page 25 in paragraph 44, where they say what they think an Internet connection record is.

Adrian Kennard: That does not really define it, I am sorry.

Mr David Hanson: That is the general broad scope.

James Blessing: That is the problem. To somebody who does not run a network, it is too vague a definition of what is wanted. When do you connect to the Internet? Where does the Internet start, for example? Is connecting to your home network connecting to the Internet or is it only when you leave that that it becomes an Internet connection record? Is your phone auto-updating its software with no intervention an Internet connection record? By definition, yes, it is. There are an awful lot of things that would have to be recorded that you do not realise happen in the background.

Adrian Kennard: I think you are referring to 47(6).

Mr David Hanson: I am referring to the background notes, the Explanatory Notes in broad terms, on page 25, saying what they are after. It is not the actual legislation, just the background notes.

Adrian Kennard: That is even worse.

James Blessing: That is the problem, because it is today's explanation, not tomorrow's explanation. Part of the reason that Internet connection records could be a problem is that, as the Bill is currently written, a Home Secretary in the future may decide to issue a notice saying that you must capture communications that happen over Skype, so you need to be able to identify which end-user talked to which end-user. It is not just that a Skype communication occurred, which we can do relatively straightforwardly, but which two end-users or multiple users were involved in that conversation. That goes into the dodgy territory of capturing third-party data because, as a service provider, I do not know which—

Q121 **Mr David Hanson:** Okay. We get the general idea. Given that the Government have established £170-odd million for this purpose, and it appears today that Virgin and BT are already planning to spend that amount, how much do you think it would cost you to meet the broad objectives that the Government are setting down?

Adrian Kennard: We are still stuck on the fact that it is a very broad objective, I am afraid. There are about three different levels of what we could be asked to do. If we already have a system that is logging some data for operational reasons, an email server that is logging emails that go through it, and we are keeping those for a few days to diagnose problems with the network, asking us to keep them for a year has some problems, but technically it is relatively straightforward and does not cost a fortune. There is a second level where we might have equipment that can be convinced to create some logs but does not at the moment, and that is a bit more work. The third level, looking into the data as they pass through our network—where we are not the service provider for an email; where something is just passing through our network—is massively more expensive. It would

double or triple our operational costs to have equipment that can look into the data as they pass through our network and extracts new information and logs it. The Bill has the scope to ask for that.

Mr David Hanson: I understand that you are a small provider. I do not know what that means in general terms, what your turnover is or how many contracts you have, but if the Government demanded that of you, how would you be able to deliver it, in terms of finance or—

James Blessing: Having vaguely sketched it—because I am a network engineer and it is sometimes an interesting exercise—in my bit of the business, which is the fixed line, not our parent company, our turnover is about £7 million. We have 40,000 or 50,000 end-users, so we are small in the grand scheme of things. You are looking in the order of £20 million to £30 million if I have to replace so much hardware on my network because it is not designed to do that; it does not have logging capability.

Mr David Hanson: Presumably if the Government do not facilitate your service doing it but do for BT, if I wished to be a child abuser, a criminal or a bank robber, I would use, with due respect, a smaller provider.

Adrian Kennard: That is a very specious argument, I am afraid. There are so many ways that anybody who is up to no good can bypass all this. They have no reason to go after a small provider. You cannot really trust that a small provider is not being monitored. It is possible that BT would be ordered to do some monitoring in the backhaul network that we, as a small provider, use. You cannot trust that monitoring is not going on somewhere in our service; it is just that we are not being asked to do it. Anyway, there is no need to. You just use any of the means to bypass this, such as Tor. At the moment even with things like iMessage you will not be able to see what is being communicated. Why would they bother trusting what a small provider says?

Q122 Mr David Hanson: The final point from me is in relation to access by the police. You will have heard other larger providers raise some points about access. How do you feel that would work in practice? Is what is suggested feasible? Do you have concerns about that or are you happy with the proposals?

Adrian Kennard: All this is about providing useful information to the police. The access is mostly a normal RIPA request, although there is the filtering facility and we still do not quite know what that will do. I am very concerned. We have experienced RIPA requests as an ISP, mostly about telephone numbers and some about Internet addresses. We have also experienced it as a victim of crime, when the police have been making requests of other providers to try to find our stolen equipment. Generally, we find that they struggle, even with modern communications. We had a case when one of our staff had to be an expert witness in a court case just to explain how phone numbers work, because they do not work in a simple way any more. My Bracknell phone number rings my mobile, my desk phone and my office phone. I seriously doubt, with that level of understanding, even with expert help, that the police will be able to make use of any sort of Internet connection records. Even experts in the industry can have trouble keeping pace with the innovation and changing trends in usage. I do not think it is going to work well.

Mr David Hanson: Is the single point of contact officer—

Adrian Kennard: They are still not going to understand it enough.

James Blessing: Having dealt with a lot of single point of contact officers, they all have the right motives at heart and they are all trying to do their job. The problem is that they are policemen first, or other types of investigator. They do not necessarily understand the results. They also do not necessarily understand the implication of providing slightly wrong information. We have had a number of cases where the time zone was missing on a request; we get a request for a particular IP address asking who was using this IP address at this time and we reply saying, "At that time, it was that". Then they come back saying, "It could not possibly have been then". Then they work out that the time zone that they had recorded it in was in the US, and that was missing. It is little things like that. Until they do it for the first time, there are going to be a lot of mistakes. The filter may exacerbate that in the short term. Long term, it should make it better, but there is a massive requirement for training and support for the police and the single points of contact to be able to use it. There is an awful lot more work than has been put in and I do not see any funds in the Bill for that.

Adrian Kennard: I am also a bit concerned about how useless this information is going to be even when it is correct. One of the examples that has been touted by the National Crime Agency and the Home Office is about the possibility of a missing child and them wanting to get data about who the child was communicating with. They did not seem to realise that a mobile phone operator is going to be able to say, "Yes, that phone has been connected to Twitter 24 hours a day for six months since it was bought", but it does not tell you, "No, they looked on Twitter or they communicated with a friend on Facebook", because—

Mr David Hanson: It might do.

Adrian Kennard: No, it is going to tell you that Facebook has been connected 24 hours a day. That is how it works. Social media and messaging applications maintain a constant connection to the service provider. They do not wake up and say, "I have sent a message". You will find far more information about the missing child by asking their friends, because they tell everyone on social media. The ISP will not be able to tell that they chose to speak to someone at two o'clock.

James Blessing: On the comment I made before about when someone connects to the Internet, if you look at your phone now you will find it has updated your Facebook feed automatically in the background every few seconds. It is constantly doing it. You can tell that someone has a Facebook account, probably—

Adrian Kennard: But that is about it.

James Blessing: You do not know which Facebook account they are using, and you do not know whether they are actively using it or whether it is just that the software is installed and running. That is the best you are going to do in that situation.

Suella Fernandes: To follow up that point, you are aware that there have been very large-scale police operations that have been successful in large part because the law enforcement

services had access to communications data or interception evidence. The Internet connection records can really help to provide a basis for further investigation, which can be critical.

James Blessing: Yes. I spent a couple of hours on Thursday morning helping a SPOC do some more research because they were not quite sure of what they had and they needed more evidence. I understand that completely. The problem with this is making sure we capture what is needed by law enforcement in a way that makes sense, so that it can interpret the information we provide securely and safely. It is not about not doing it at all. It is about asking what you actually need at the end of the day. The other problem you potentially are going to create is that, if you record all the records of every single connection that you are doing, stuff will be lost in the noise. You will start relying on data and say, "They were connected to there", when their phone might have been left in their bedroom turned on while they were somewhere the other side of town.

Q123 Suella Fernandes: I just wanted to make that point. A second question is about the security measures you use with the data that you have. Can you give us a bit of an idea of which mechanisms are effective for you?

James Blessing: As a company, we take credit cards, and there is a standard that we have to follow for that, which basically means the information is stored in an encrypted database with multiple levels of firewall protection. As far as we are concerned, if we were to do this, I would put the same level in place. I would do some checking. Part of the reason the filter is a concern is that you have to give third-party access to it, and it might need some engineering work to make sure that only trusted parties can access it, but that is a different issue.

Suella Fernandes: You say that firewalls and personal vetting systems are sufficient.

Matt Warman: Very briefly, it seems that a lot of what you have been saying is that there is a whole load of stuff that we may or may not need to record—some of that stuff about "When is your phone connected to Facebook?" All that I absolutely understand, but once we have nailed down the definitions that ceases to be your problem.

James Blessing: Yes. Nail down the definitions and everyone starts going, "Right, okay, now I can work out how to deal with it".

Lord Strasburger: I want to clarify Ms Fernandes's question. I presume she was referring historically to communications data derived from telecommunications rather than from the Internet. What you are saying—the view you are expressing, if I am hearing you correctly—is that the efficacy of the Internet communications data that are going to derive from Internet connection records is doubtful, as opposed to telephone communications data.

Adrian Kennard: Telephone communication is very clear-cut; it is the building block of the telephone network that telephone calls are made and everyone understands the concept and it is very clear. The Internet is not like that. Devices are constantly talking, constantly communicating with lots of different services all the time. Connections can stay running for days, months or years, and that is one connection. The usefulness of this is much more limited, with a lot more noise. It could be misused easily. It is very easy for someone to

appear to be accessing services they have never heard of. I did a blog post today, and anyone who reads it will find they have accessed Pornhub because there is a tiny one-pixel image in the corner. They do not know that, but it will appear on the Internet connection record if they access my blog. That was deliberate, but there could be lots of things on websites, advertising networks and so on, that will create all sorts of misleading and confusing data even without someone trying to be misleading. As I understand it, in Denmark they had nearly a decade of trying to capture sessions on the Internet and abandoned it because they found it not to be very useful for law enforcement.

The Chairman: Ms Fernandes, did you want to come back on that other one?

Suella Fernandes: No. I meant how people are sending emails, what they are sending on the Internet.

The Chairman: I meant on the Information Commissioner.

Suella Fernandes: You are right; it was to follow up Lord Strasburger's presumption about what I meant in my question. I lost my train of thought. The question I wanted to ask initially was whether you think that firewalls and personal vetting services are sufficient for maintaining security.

James Blessing: Let us get this right. If operated according to design by the right people in the right way, yes. The difficulty is that operational procedures can drift away from perfect. It would not surprise me if there was a breach of the data stored in an Internet connection record at some point. It is not a question of if; it is a question of when. There will be a breach.

Adrian Kennard: Bear in mind that even the NSA, which has huge resources, had Snowden. It does not matter how well we do this, somehow someone will lose data; they will be breached and it will potentially be sensitive personal information.

James Blessing: As an example, the Home Secretary has possibly made herself a target for people who want to show that this is a bad thing to do; they may well try to go after her home service provider because they think that is a good thing to do.

Q124 Stuart C McDonald: You referred a couple of times in passing to filter requests. What is your understanding about how these are going to work, and what concerns would you have about their operation?

James Blessing: In theory, the filter is being described as a way of restricting the information recovered. That means that an automated system must be doing the requesting of the data capture from the service provider and then presenting them to an individual. That means we have to allow third-party access to our systems, which is a potential risk. In theory, it would mean that the data was less open to fishing because you are only getting back specific results, but potentially there is a whole new construction of requests that people could start making, saying, "Who has visited Pornhub recently?" and Adrian's blog, and then putting that together, because it might be an interesting subset of people to go and do something else with. In some ways it is a good thing and in some ways it is a concern, because, again, the details are very limited.

Stuart C McDonald: It is the Home Office that would build the filter; is that right?

Adrian Kennard: I do not think it is specified.

James Blessing: Again, part of the problem is that it is not clear who operates which bit of the filter and how the filter would work. As far as I can tell from the information provided so far, it seems to be implying some sort of API access.

Adrian Kennard: Automated.

James Blessing: It is an automated access. Basically, a request comes in and it returns that information. How that happens in real life is not clear.

Q125 Lord Henley: Can I turn to Clause 189 and the ability of the Home Secretary to impose certain conditions on relevant operators and that these would come in the form of technical capability notices? I would like to hear what your views are on the ability of the Home Secretary to impose such a notice. How do you think your customers are going to react?

Adrian Kennard: My biggest concern is the removal of protection on communications. This comes down to the whole issue with iMessage, to some extent, in that it is end-to-end encryption at the moment. If providers are required, even secretly, to remove that protection, it removes all trust in those providers if they are offering a secure communications service but at any time they could be subject to an order that makes it not secure. That is a reason for companies to avoid being based in the UK and for customers to avoid UK companies. Encryption is a good thing; it is what keeps us safe from the very real threat of cybercriminals. If you got every communications provider in the UK, and even every foreign communications provider, to have this capability and to remove the protection they have provided, that still does not stop people, including criminals, communicating secretly. There are applications that do the encryption for you on your own machine when you send messages so that the provider cannot remove it. It is even possible to send messages that are completely secret—GCHQ could not get the information from those messages ever—just using pen, paper and dice. You could ban all computers and it would still be possible for people to communicate secretly. It is undermining trust and not solving any problems to tell operators they have to remove protections.

James Blessing: Most of the stuff is covered. The issue again is that it is not the Home Secretary who would be requesting that. It would be law enforcement because it needed to do something, which always comes down to this: most service providers are willing to help law enforcement because, at the end of the day, we are part of a wider society. Forcing someone to go and break something tends to mean there has been a disagreement about doing something in the first place, and that is not a good place be to be.

Adrian Kennard: I have one other concern to do with the definition of communications provider. I have another hat today. I am a manufacturer, a UK business, making equipment that we sell round the world—a firewall router that would go in a small office. I am very concerned that there is the possibility that we could be asked to put in back doors or remove encryption as part of this. I think we would have to move the business out of the UK if the Bill goes through as it is at the moment.

Q126 Lord Henley: Now we turn to oversight and the proposed Investigatory Powers Commissioner. How do you see your relationship with him or her, and what changes would be appropriate when that office is created?

James Blessing: It is good that additional oversight is being created and put in place. That is always a useful thing to have. It is not clear from the Bill how independent a voice that person would have considering they are going to be appointed by the Home Office, pretty much, and they would be a judge. I am a bit sceptical that they would be as independent as their job title would lead you to believe.

Adrian Kennard: Yes. I have similar concerns.

Lord Henley: Finally, my Lord Chairman, I have one other question for clarity. I think it was Mr Blessing who implied that the costs imposed by the Bill, if enacted, could be such that his business would have to spend something of the order of four times your annual turnover.

James Blessing: Yes. Basically, the reason for that is that we have grown over time from a small organisation. We build the network small and then grow it, so there are no logical places within our network to do all the stuff that is required. We would have to go through replacing lots of pieces of hardware and upgrading them and their capabilities.

Lord Henley: Would that same figure, a factor of four, be as true both for small providers such as yourself and your membership as for some of the larger ones?

Adrian Kennard: It is difficult.

James Blessing: It is difficult. There are certain service providers where, because of their business model and the way they have built their network, it would be easy to do and it would not cost that much, but there are others in our situation where it would cost that. There are probably others where the multiplier is even higher. It will be variable because every network is different.

Lord Henley: The figure you were giving was one from your own experience with your own business.

James Blessing: Yes.

Lord Henley: It would not necessarily be true of all your members, but it might be higher or lower.

Adrian Kennard: Our business is different yet again. As James was saying, every ISP does things differently; it has different networks and will have different costs in doing things. In our business we make those FireBrick products and sell them to ISPs and use them in our network. It is entirely our own R&D in the UK and we have spent millions developing it. If we now have to change that to do different things, it could cost millions, or we scrap all our own work and buy in third-party kit, which would also cost millions. We would have to make major changes to do that.

Matt Warman: You talked about your fear that the Bill might ask companies to stop end-to-end encryption or that it might ask for back doors to be inserted. We have had the Home

Office in front of the Committee saying that is not the case. The Home Secretary has said that on the Floor of the House. Are you saying that you do not believe them when they say that—

Adrian Kennard: No. But put it in the Bill if that is the case. It is as simple as that.

Matt Warman: The end of my question is whether you would simply like more clarity.

James Blessing: The issue is not the current Home Secretary or Home Office. That is the problem. It is that you have put it in the Bill; it is there. There are two things. It is in the Bill and therefore we are looking at it saying, "Technically, someone could do that". More importantly, someone outside the UK who trades with the UK will look at the Bill and say, "That technically says that they could do this".

Adrian Kennard: And "I am not going to deal with them".

James Blessing: I have two choices: this company in the UK and this other one outside, and I am a bit worried about that, so I will use the other company instead.

Adrian Kennard: We have already seen how putting too much scope in a Bill can be abused, with councils using RIPA to spot people going to a school outside their catchment area. I am sure the council thought, "We have got this power and we would be negligent not to use it". I suspect future Governments, Home Secretaries and Secretaries of State might well say, "We have got this power and we should be using it". Anything that is possible could happen. It is worrying.

The Chairman: On that very interesting note, thank you both very much. It was a very useful session, very informative. Thanks very much for coming along.

Dr Paul Bernal, Lecturer in Information Technology, Intellectual Property and Media Law, School of Law, University of East Anglia (QQ 76-93)

Evidence heard in public Questions 76-93

Oral Evidence

Taken before the Joint Committee

on Monday 7 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Bishop of Chester, Lord Henley, Lord Strasburger.

Witness: **Dr Paul Bernal**, Lecturer in Information Technology, Intellectual Property and Media Law, School of Law, University of East Anglia, gave evidence.

Q76 The Chairman: We extend a very warm welcome to our four guests this afternoon. We are very grateful to all of you for coming along on what is a hugely significant Bill that is going through Parliament—the Prime Minister called it the most important of this Session. Thank you very much indeed. As you probably know, the procedure is that I will kick off with a question or two, and then my colleagues will in turn ask you various questions on different aspects of the Bill that I think you find very interesting. If, when I ask a question of an individual, he wants to preface his remarks with a short statement, that is entirely up to him. I turn first to Dr Bernal. After you have answered, colleagues will be able to come in. What are your views on the draft Bill? Does it deliver the transparency on investigatory powers that you have particularly called for?

Dr Paul Bernal: Perhaps the best way to put it is that it goes part of the way. As far as I am concerned, it is good to see everything in one place, or almost everything—some bits are clearly missing—but for proper transparency we do not need just the Bill; we need the process to work properly as well. I would have said in my introductory remarks, had I made any, that the timetable makes it very difficult to get as much scrutiny as we would like; we have been called here very rapidly, and you have only a few weeks to do this. For transparency to work properly we have to have the chance and time to put our analysis into action. It is a bit difficult to do that.

One other thing I would say about transparency is that certain terms are used and expressed in a way that is not as clear as it could be. There are terms like "bulk powers" when we do not really know how bulky "bulk" is, if you see what I mean. For things like Internet connection records, it has taken some time, and we are still only part of the way there, to tease out what it really means. From that perspective, it is good to have it all in one place, but the process needs to be stronger. We need to make sure there is enough time to do it, and I am not sure you have as much of it in this Committee as you would like—perhaps later on there will be time—and we have to tease out some of the terms more accurately.

There is one other aspect. Some of the things in the Bill will become dependent on codes of practice and similar things that go with it. For transparency's sake, so that we understand what is going on, those codes of practice need to be put in a form that we can all see prior to the final passage of the Bill.

Q77 The Chairman: You have touched on the second question I was going to ask, so I will raise it now. You mentioned the codes of practice, which are hugely important in all this. What do you think the legal status of those codes might be?

Dr Paul Bernal: The legal status of the codes depends a little on how the final Bill turns out. From our perspective as legal academics, the key thing about codes of practice is not so much their legal status, which, depending on how it is set out, will be clear, but the extent to which they are also subject to the level of scrutiny and attention that the Bill itself is. It is easier to pass a code of practice through a small statutory instrument than to pass a whole Bill with full-scale scrutiny. We want to make sure that the codes of practice, which can be the critical part, get the same degree of scrutiny and attention both from people like us and from people like you.

The Chairman: With regard to the timetable, of course the issue that affects both this Committee and Parliament is, as you know, the sunset clause in the current legislation. Parliament has now laid down the amount of time we have. We certainly ensured that we gave ourselves extra and longer sessions, including in and around Christmas, and I am quite convinced that both Houses of Parliament will give it very thorough investigation, as indeed they should, but the point has been made. Does anybody else wish to speak on those issues?

Professor Sir David Omand: If I may make two remarks, the first is to stress the importance, in my opinion, of the Bill as the culmination of 500 years of history. It has taken 500 years to put the secret surveillance activities of the state under the rule of law. For centuries we had the royal prerogative being used in secret. Parliament passed the device of the secret vote but asked no questions. We had executive regulation in the last century, and for the past couple of decades we have had a patchwork of provisions in legislation, so all that secret activity was lawful but not understood. This Bill now places it under the rule of law; it will be comprehensible to the citizen. I cannot overestimate the importance of the Bill.

The second point is to agree strongly that it is in the codes of practice that the public will find it easiest to understand what is going on, rather than in the technicality of the Bill itself, so the codes are very important. Schedule 6 to the Bill sets out very clearly what the status of those codes will be. They will have to be presented to Parliament, along with the enabling statutory instrument.

The Chairman: Professor Anderson or Professor Ryan, are there any comments you would like to make at this stage before we move to other questions?

Professor Ross Anderson: I believe you will be asking me in due course about Internet connection records.

The Chairman: We will.

Professor Ross Anderson: It would be great if, in addition to having codes of practice, we had very much greater clarity on definitions. I will discuss Internet connection records, but there are other things that are not really defined at all, from the great concept of national security down to some rather technical things. I hope that clarification comes out during the Bill's passage.

The Chairman: You think such definitions should be on the face of the Bill.

Professor Ross Anderson: Yes.

The Chairman: Professor Ryan, are there any initial comments you would like to make to the Committee?

Professor Mark Ryan: Just on questions 1 and 2?

The Chairman: At this stage, yes, because there will be other more detailed questions, some of which will probably be directed to you personally as well, but at the beginning of the session would you like to make any general comments?

Professor Mark Ryan: The comment I would like to make about transparency is that this seems to be such an important area that the kind of oversight proposed is not enough. One would need more quantification of the sort of surveillance that takes place. Of course, I am aware that surveillance has to be done in secret, but I believe that the quantities of surveillance and the nature of surveillance can be disclosed to people without compromising the secrets of the surveillance activity. That seems to go more towards transparency and is much stronger than mere oversight, so I believe there should be more of that.

Q78 **Dr Andrew Murrison:** You have covered a huge amount of ground in about seven minutes. You hit the nail on the head in terms of definitions and the need to ensure that codes of practice and statutory instruments are sufficiently transparent and that scrutiny is of the utmost. I am interested to know how you think scrutiny and transparency can be improved other than through the normal process of laying statutory instruments before the House, because I sense from what you said that you feel that the Bill, which talks about SIs and codes of practice, is not sufficient in that respect.

Dr Paul Bernal: I would not say exactly that it is not sufficient. What I am interested in is getting as much scrutiny as we can. In order that we can understand the Bill we need to have the codes of practice at the same time, at least in draft form, so that they can be examined; frankly, to understand some of the powers in the Bill without a code of practice is very difficult, particularly on things like bulk powers and Internet connection records. We will talk a lot about Internet connection records later, but they are defined in such a way that it is unclear on the face of the Bill exactly what they will mean in practice.

Historically, not as much attention is paid to statutory instruments by the House. You do not spend as much time passing them as you do Bills; you do not have Committees scrutinising each of the statutory instruments at the same level of detail.

Dr Andrew Murrison: But it is worse than that, is it not? This is a very rapidly moving field, so you cannot reasonably lay all the codes of practice and anticipate all the SIs at this time, since 12 months down the line there may be yet more to come.

Dr Paul Bernal: Yes, and that is a fundamental problem with any kind of Bill in this area. I do not know whether there would be a mechanism to produce better scrutiny of the codes of practice, but attention should be drawn to the fact that this will be important as it continues. It needs constant attention, not just at the moment we pass the Bill.

The problem with the Regulation of Investigatory Powers Act was that, although it got a lot of attention at the time, the things that gradually built up to create the confusion—chaos is not quite fair—for people about the overall regime, and which stimulated the need for this Bill, were not sufficiently attended to over the years as things happened. We need to make sure that does not happen this time around.

Dr Andrew Murrison: Do you think a sunset clause would help? We are replacing one sunset clause with another. Is that inevitably where we are going to be led?

Dr Paul Bernal: Frankly, in this area you need sunset clauses in almost everything, because the technology moves and the behaviour of people changes. The overall situation changes. You need to be able to review these things on a regular basis, and a sunset clause is one of the best ways to ensure that happens.

Professor Ross Anderson: Last time around how we dealt with this was that, in the run-up to the passage of the Regulation of Investigatory Powers Bill through Parliament, a number of NGOs organised a series of conferences called Scrambling for Safety, and afterwards various statutory instruments were laid before the House. We are proposing to do the same again. The first Scrambling for Safety workshop is to be held at King's College London on 7 January from 1 pm to 5 pm, and all members are of course very cordially invited. We anticipate that it will be the first of a series that will enable engineers, lawyers, policymakers and others to dig into the meat of what is going on, exchange views and push the thing forward.

Q79 Suella Fernandes: Based on your expertise, would you set out briefly the nature and extent of the problem or threat we are facing when it comes to the use of this technology?

Professor Ross Anderson: The problem with the use of surveillance technology is that, if it is used in ways that do not have public support, it undermines the relationship of trust between citizens and the police, which has been the basis of policing in Britain for many years. Sudden revelations like Snowden are extraordinarily damaging because they show that the Government have been up to no good. Even though the Government may come up with complicated arguments about why bulk equipment interference was all right under Section 5 of ISA and so on, it is not the way to do things. There was a hearing in the Investigatory Powers Tribunal last week on that very issue.

There are other issues. The first is national leadership. If we go down the same route as China, Russia, Kazakhstan and Turkmenistan, rather than the route countries such as America and Germany have gone down, there is a risk that waverers, such as Brazil and India, will be tempted to follow in our wake. That could lead to a fragmented IInternet, with

extraordinarily severe damage for jobs, prosperity, international stability and, ultimately, the capability of GCHQ to do its mission, because if you end up with the IInternet being partitioned into a number of walled gardens, like the Chinese or Iranian ones, they will be very much less accessible to the intelligence agencies.

In addition, if the powers are abused, or seen as capable of being abused, there could be exceptionally serious damage to British industry. If people overseas come to the conclusion that, if they buy a security product from a British firm, it may have a GCHQ-mandated back door, they will not buy it; they will buy from a German firm instead. This is where the rubber hits the road when it comes to overreach in demanding surveillance powers.

Professor Sir David Omand: On the other hand, my advice to the Committee would be that this Bill contains the basis of the gold standard for Europe. This is how you get both security and privacy in respect of freedom of speech. The interplay of checks and balances and oversight regimes means that none of what Professor Anderson has described needs to happen. Of course, with a malign Government and agencies that flouted the law it would be possible to have abuses. I do not believe that either is likely, and certainly the provisions in the Bill allow this House to maintain very strict control of the Executive in its use of these powers.

Professor Ross Anderson: With the greatest respect, the reaction of America and Britain to the Snowden revelations has been somewhat different. In America people have rowed back in all branches of government. For example, President Obama has, simply by executive order, commanded the NSA to minimise the personal information of unaffected foreign nationals, like us. The legal branch has seen to it that, for example, national security letters, which used to be secret for ever, are now disclosed after three years, and Congress failed to renew provisions for the retention of American citizens' communications data. All branches of government have pushed back and sent a solid signal to the world that America cares about privacy and the proper regulation of its law enforcement and intelligence services. If the reaction from Britain is different, even if powers are not abused, it still sends a signal to the Brazils, Indias and, may I say it, the Kazakhstans. We do not really want that.

Q80 **Bishop of Chester:** A sunset clause is the nuclear option of legislation, but reading the Bill I am wondering how there is a process of inbuilt review, because the scene is changing so fast. There is a technical supervisory board bringing together stakeholders and so forth. Should there be an inbuilt power to renew the provision? That has been in some previous terrorist legislation. There has not been a formal sunset clause, but there has been a renewal motion. That would force Parliament to review what is happening, because for the legislation to continue there would have to be a renewal notice.

Professor Sir David Omand: Of course, it is Parliament's prerogative to put in such a provision. My experience in the public sector is that it should be done very sparingly, because it may turn out that at precisely the moment you have to legislate afresh, as with DRIPA, Parliament may not actually want to legislate afresh. One concern I had was whether the definitions in the Bill were sufficiently robust to deal with technical change. Having studied them, I am as confident as I can be that they avoid hostages to fortune, so your House will not discover in a couple of years' time that a different Bill is needed because the technology has moved on, but that will need to be examined by detailed scrutiny.

Q81 Shabana Mahmood: My first question is to Professor Anderson and then his colleagues. We have two competing narratives of the Bill: one that these are significant new powers and major changes, and the other that it is just codifying current provisions and bringing them more obviously and explicitly within the rule of law, as Sir David suggested. Professor Anderson, what is your view as to which of those narratives is more accurate?

Professor Ross Anderson: The Bill has been marketed as bringing in only one new power, namely Internet connection records, but it does many other things as well. For example, when the Regulation of Investigatory Powers Bill passed through this House and became an Act, one of the things we lobbied for and secured was the provision that if the agencies wished to command somebody to decrypt something, or hand over a cryptographic key, there should be special safeguards. The City of London did not want a rogue superintendent, perhaps in the pay of a criminal gang, to approach a 24 year-old assistant shift supervisor at a bank's data centre somewhere in east London and command him to hand over the bank's master signing key. Therefore, the provision was made that the production of a cryptographic key had to be demanded by a Chief Constable in writing and the letter had to be presented to a main board director of the bank. There are many provisions like that which appear to be swept away by this new legislation. Parliament must realise that the arguments are just as strong today as they were then; otherwise, how are you going to persuade international banks that London is a good place to do business? Some banks already had issues last time around.

My second comment is that a number of things that were previously done secretly were made public only in the run-up to this Bill, which enables the Bill team to say, "This is old stuff. We knew about it already". I refer members to the Investigatory Powers Tribunal hearing and the long arguments therein about whether an ISA Section 5 warrant could be used for bulk interception or only targeted interception. There are many technical aspects like that.

Thirdly, although the Internet connection record is ostensibly the new thing in the Bill, it actually gives very much greater powers than have been advertised; rather than just helping IP address resolution, it enables a policeman to say, for example, "We have these two bad people. Show us all the websites they both visited last month, and tell us the names and addresses of everybody else in the world who visited the same addresses". That is an extraordinarily powerful capability. It is the sort of thing that Internet service companies use to fight spammers, phishermen, click fraudsters and so on. Those of us who have worked in that field know how powerful it is and tend to be of the view that it should be classified along with intercept. If we are to have a special higher burden for intercept warrants, that higher burden should apply also to complex queries that are made on traffic data.

Shabana Mahmood: Have you done any analysis of powers advertised one way but which, as you suggest, lead to, say, five extra things? Have you made some sort of qualitative analysis to back up the examples you are helpfully giving us?

Professor Ross Anderson: The qualitative analysis basically comes from experience working at Google on sabbatical four years ago with the click fraud team. Knowing that such inquiries are extremely powerful, and talking to colleagues at Yahoo and Facebook recently, there is general concern that, if you allow people to make complex queries like that, it is up

at the level of a box of fancy tricks; it is not the sort of stuff you want to let an ordinary policeman do without supervision, because it can be used to do some very bad things.

Professor Sir David Omand: The Bill does not provide for ordinary policemen just to request that. There is a mechanism for a single point of contact and independent agreement before data can be acquired. I do not recognise either of the extreme cases Professor Anderson puts forward, but no doubt the Committee will need to investigate that further.

Dr Paul Bernal: If I may add something in response to that, there is something missing in the idea that these are either new powers or old powers. People's behaviour has changed fundamentally. The Internet, which was a medium used for communications—in the old-style idea of communications—is now used for almost everything else: shopping, dating, research and that kind of thing. The same power applied in a different situation gives a significantly higher level of intrusion than we have ever seen before. It is not like listening to phone calls, reading emails or things like that; it is like following people down the street while they shop, looking at the books they take out of the library and things like that. Without even changing the law, you are significantly changing and increasing the level of intrusion. It has lots of different implications, not just in terms of the balance of privacy and things like that but all the other rights we normally think of. Our expectations of privacy are different from those we had in the past. In a way, it comes down to the idea of how the law is going to change and how we need to take things into account. We need to take into account not only developments in technology but the way people's behaviour changes in relation to that technology; for me, in effect, that is the biggest increase in power. It is not that there is a new power built into the Bill, but because we use communications so much more extensively it is a much more intrusive thing to do any kind of Internet surveillance.

Professor Sir David Omand: That is why the Bill defines event data, Clause 193, in a conservative way, not taking modern metadata but imposing on the rather fuzzy reality some precise definitions, to minimise—it cannot be avoided completely—the kind of case Dr Bernal referred to. Inevitably, if you impose strict definitions on fuzzy reality, you will occasionally get hard cases. Those will exist in this world. As we know, the difference between dangerous driving and driving without due care and attention means that sometimes cases fall on the wrong side of the line, but the old adage that you do not make law by hard cases still applies. I commend to the Committee the way that the Bill has not expanded the definitions of communication data in defining event data.

Q82 Shabana Mahmood: That is helpful. You touched briefly in your previous answers on my final question, which is about future-proofing the Bill to take account of the pace of behavioural and technological change. We had evidence from officials from the OSCT. They were very bullish and confident that the changes in relation to Internet connection records in particular meant that it was sufficiently future-proofed. Could we have your comments on that?

Professor Ross Anderson: I have two main comments. The first is from the viewpoint of the long term—20 years out. We are simply asking the wrong question. The right question is: what does the police service look like in a modern technological society? Is it completely centralised? Does it go like Google? Do Ministers take the view that a chap sitting in Cheltenham can learn more about citizens in Leicester than a bobby on the beat in

Leicester? What sort of society does that become? This is a much broader conversation than just about who gets access to whose mobile phone location trace when.

The medium-term issue, which I think will become acute over a period of five to 10 years, is that the real problem is a diplomatic one. The real problem is about jurisdiction and how we get access to information in other countries, specifically America. America is where the world's data are kept. If they are kept in Finland or wherever because of cheap electricity, usually they are still controlled by a US company. There are some exceptions—Korea, Japan et cetera—but this is largely about how we get access to American data.

That means, like it or not—and many people are beginning to come to this conclusion—that the real fix for this is a cyber-evidence convention, like the cybercrime convention. That will involve diplomatic heavy lifting and an agreement, perhaps initially between America and the European Union, with other willing countries joining later as they wish, that provides a very much faster service for getting at stuff than the current mutual legal assistance treaties. For that to work, there are three things we almost certainly have to have. The first is warrants signed by judges, because that is what America expects. The second is transparency, which means that if somebody gets wiretapped you eventually tell them—when they get charged or after three years or whatever. The third is jurisdiction, because the real bugbear for companies like Google at the moment is that a family court in India gives it a warrant saying, "Please give us the Gmail of this person in Canada", who has never been to India. How do you simultaneously employ engineers in India and give privacy assurances to your users in Canada? That is why at present all this stuff gets referred to lawyers in Mountain View. That is the real problem, and it is time the Government faced up to it.

The Chairman: Professor Ryan, do you want to say something regarding an earlier point?

Professor Mark Ryan: I want to go back to the question of whether these are new powers or existing ones. Following what Dr Bernal said, one of the very huge powers that exists in the Bill is bulk equipment interference—that the state can interfere with people's computers on a bulk scale—which means that people who are not guilty of any crime, nor even suspected of any crime, may have malware put on their computers by intelligence services to collect vast amounts of data on innocent people in a kind of funnel, so that eventually criminals can be caught, but the people who are being subjected to that are not criminal at all. That seems to me to be an extremely dangerous thing in a free society. I do not think that the kind of oversight proposed in the Bill goes anywhere near being able to control that type of activity.

Professor Sir David Omand: The bulk equipment interference warrant can be sought only by the intelligence agencies in order to acquire intelligence relating to individuals outside the UK for the purpose of national security. For the sake of clarity, the Bill already restricts that.

Q83 Lord Strasburger: Sir David, your career was spent in senior positions in the Civil Service deep inside the security establishment, which probably makes you, of the panel, specially qualified to answer my question. It seems that over the past 15 years decisions were made behind closed doors to introduce several of the most intrusive and least overseen powers in this Bill without bothering to seek Parliament's approval. Why was it considered acceptable in

a democracy to bypass Parliament and introduce large-scale and highly controversial surveillance powers without Parliament's explicit approval?

Professor Sir David Omand: I can only hazard an answer, which is that the legal regime under which previous Governments operated for the past 20 years, since the 1980s, was what I would describe as legal compliance; in other words, if it could be done lawfully under existing powers that Parliament had passed, Ministers would authorise such activity, after due legal advice, regardless of party—this is not a party political matter—in the interests of national security, the prevention and detection of serious crime, and economic well-being arising from causes outside the United Kingdom. That was the regime.

It was really when the Investigatory Powers Tribunal took the case and reported that the Government's activity, in particular GCHQ, might be regarded as lawful under the individual statutes but failed the rule of law test because it was not clear, as your question implies, to the public—

Lord Strasburger: Or to Parliament.

Professor Sir David Omand: Or to Parliament. This Government have taken that to heart, and the Bill is in part the result. We have moved into a new era and I am personally very glad of that. A lot of trouble would have been saved if, say, even five years ago the codes of practice—it would not necessarily have taken new legislation—on equipment interference, investigative powers and so on had all been updated to the modern digital world. For one reason or another that was not done. The shock of discovering what was happening, for very good reason—to defend the public and our security—was all the greater. I think the lesson has been learnt.

Q84 **Victoria Atkins:** I have a question for Professor Anderson and Dr Bernal. You talked a lot about privacy and, in particular, the debate in America about privacy. One thing that strikes me about the whole discussion is that very often we are focusing, if I may say so, on the worst-case scenario as to what the intelligence services and the Government will do with people's information. What are your views in relation to the computer companies that hold all this data about us? If we google a dating agency, Google will have that information. What are your views on those bodies, because to me they are very much part of the debate about privacy?

Professor Ross Anderson: Yes. I tend to take different views of different companies because of their different internal cultures. Having worked at Google, I understand and to some extent trust the culture there.

Victoria Atkins: You worked at Google.

Professor Ross Anderson: Yes, four years ago on sabbatical, so I understand it. My colleagues have worked for other companies. Fundamentally, whether you are a company that tries to be good or a company that is a bit less scrupulous, the underlying fact is that the modern economy depends on people trusting large service companies with their data, because it is so much more efficient to have 100 million people's data in a data centre than it is for everybody to be backing up their own hard drive at home and losing their photos

and everything. That trust has to be maintained. If it is lost, the consequences could be dire for economic growth and the companies concerned.

People talk about worst-case privacy scenarios, but that is how people talk; that is how the media and politics operate—they operate by stories. The human brain is optimised for stories; it is how people remember stuff. If you get the perception out there that in the UK people who offer services have to leave a government back door, or remove the encryption if ordered, or whatever, it could be extraordinarily damaging for British business.

Victoria Atkins: Does selling people's data come into that? Are you comfortable with Google's position on that, having worked for it?

Professor Ross Anderson: Personally, I do not click on ads. If you want to go to a company that does not sell data, you can go to Apple or you can go to the trouble of having everything private. For example, I take the view that, if I am sending an email that I do not mind the FBI reading, I use Gmail; if I am sending an email that I do mind the FBI reading, I use something else. That is also the conclusion to which I think more and more users generally, and young people in particular, are coming to.

Q85 **Matt Warman:** I have a question for Dr Bernal primarily. As an example of new powers in this Bill, you said it was like following someone down the street and seeing which shops they go into. It strikes me that we have long had the power under certain circumstances for people to be placed under surveillance and followed down the street to see which shops they might go into. Could you give the Committee an example perhaps when we get back?

The Chairman: Order. There is a Division in the Commons, so we will adjourn for 10 minutes. I am sorry about that.

The Committee suspended for a Division in the House of Commons.

Matt Warman: To recap briefly, you cited the example of following a person down the digital street under authorised surveillance, which strikes me as a digital updating of analogue powers we have already. Could you offer the Committee an example that is not simply a digital updating of existing analogue powers and is genuinely novel because it is digital?

Dr Paul Bernal: It is a very important question, and there are lots of issues related to it. There are some things that we do in the real world, or the offline world, that we feel comfortable being observed doing. We have CCTV cameras in the streets, we have them in shops, and so on. We do not have them in our bedrooms, we do not have them staring at our diaries all the time and we do not have them monitoring exactly where we walk. We get the choice: do we want to go to this place where we know there is CCTV, or that place where we know there is not CCTV? That is one of the important differences.

The thing about the Internet as it is now, particularly for younger people, is that they do literally everything on it; there is no aspect of their lives that does not have an online element. If you have a system as is proposed with Internet connection records, for example, where there is some gathering of their entire browsing habit, not beyond a certain level—I hope we will get on to Internet connection records later—at least you have knowledge

about what they are doing in every aspect of their lives. When you go to the doctor, you expect confidentiality from your relationship with the doctor when you discuss your health issues. If you visit a website to research a particular health condition, that may reveal just as much about you as you would reveal to your doctor—in fact, many times more than you might reveal, because people have a sense that they can get more intimacy by doing things on the Internet than they might even be prepared to admit to a doctor.

There is another element. We talked a little about Google and others. Given the way profiling works for almost all commercial Internet companies, and the way big data analysis works, you can draw inferences from relatively small amounts of browsing data that can then be used to infer stuff that you would otherwise keep private. An example is your sexuality. You might not want to reveal your sexuality, but big data can make a probable analysis of it with a relatively small number of places you visit on the Internet.

It goes back to the question about whether we are looking at extreme cases. We are looking at extreme cases in some ways, but we are also looking at very ordinary cases. What we all do on the Internet has an impact on credit ratings, insurance premiums and things like that. They can be based on very basic information that can be gathered about how we behave.

I am sure David will say that safeguards are built into the Bill so that it can be used to do only certain things, but that is not really the whole story for two reasons. One is that data, wherever they are and in whatever form, are vulnerable in many different ways. The example that comes most readily to mind, because it is so recent, is TalkTalk having been hacked, and holding exactly the kinds of records that we are talking about. That information is ideal for ID theft, credit card fraud, scamming and things like that.

If we gather those Internet connection records, we are basically creating a very targeted database, which says on the front, "Hack me, please, if you want to get ideal information for these kinds of crimes". We need to be careful not just about what we think the Government are going to do. Like David, I trust to a great extent our security services and police, but we are creating something that can be misused by other people, not just by them. There are many ways in which that can happen.

Q86 **Suella Fernandes:** In terms of legality, the issuing of warrants is subject to the test of it being necessary and proportionate. In light of that, what is your view on its compatibility with proportionality as required under the ECHR?

Professor Sir David Omand: Proportionality and necessity are in the Bill. They are written in, as they are in the current legislation. Dr Bernal's examples were very good ones of why digital mass surveillance is a thoroughly bad idea. Thankfully, it does not happen now, and under the provisions of this Bill it could not happen in the future either. The question that I suggest the Committee really needs to address is how proportionality is assessed—precisely your question—not just in relation to the granting of a warrant but the whole process through which the selection of material for examination by human beings—the analysts—takes place. The IPT, the independent court, has examined this; senior judges who oversee interception have examined it, and they are satisfied that the current procedures are consistent with the Human Rights Act, Article 8 and thus respect privacy. Equally, there is no reason why the provisions cannot be applied in practice in ways that remain consistent.

The decision on proportionality and necessity rests with the person signing the warrant. The Home Secretary has made her view clear in the Bill. I am disappointed that she decided that she had to sign police warrants and that they would not go direct just to the senior judge for approval, which was our recommendation in the independent review commissioned by the former Deputy Prime Minister, and that would be more consistent with David Anderson's review. I strongly believe that the Home Secretary or the Foreign Secretary, as appropriate, should sign the warrants relating to national security and the work of the national intelligence agencies, for which they are statutorily responsible to this House. The police service is in a different constitutional position, and I would have thought that purely police matters could go straight to the judge. It is no harm that the Home Secretary signs as well; it is just additional work.

Dr Paul Bernal: Can I go back to the question of proportionality? One of the key things is not just about the warrant to access the information. One of the key elements of proportionality is the gathering and holding of the information itself. The CJEU has consistently—even more so recently—held that the holding and gathering of the data engages Article 8, and that indiscriminate generalised holding and gathering of data is contrary to fundamental rights. That was held in Digital Rights Ireland; in the Schrems case it was part of the key reason why the safe harbour decision was invalidated. This is not because they have some perverse view that does not match with reality but that the European Court has started to understand the impact of holding all this personal data. It is not just the warrants—to a degree, I agree with David about the warranting process; it is the gathering of the data that I disagree with, particularly the way Internet connection records are set out. All this data seems to me to be gathered on the assumption that that is all okay and it is just the accessing we need to deal with. I cannot see how this law would survive a challenge in the CJEU on that basis.

Professor Sir David Omand: I very strongly disagree. I am not a lawyer, but it seems very clear to me that the Schrems and the Digital Rights Ireland judgments do not bear on the point that has just been made. Those judgments did not consider the question of proportionality of collection and selection, which is not indiscriminate collection of data willy-nilly. You might want to take advice on that.

Professor Mark Ryan: I want to comment on the bulk provisions of the Bill, because they allow for the collection and automatic processing of data about people who are not suspected of any crime. Therefore, I do not think it is correct to say that this is not a recipe for mass surveillance. It is the processing of data about everybody, and in my opinion that is mass surveillance.

Professor Sir David Omand: But it is not processing data about everybody.

Q87 **Baroness Browning:** We have covered quite a bit of my question about definitions. Clearly, we have differing views on the panel. Sir David, in your evidence to the Science and Technology Committee I believe you suggested that somehow you would never get a perfect definition, and in the absence of that a pragmatic approach should be taken. Do you want to identify the balance between being safe and being practical?

Professor Sir David Omand: The starting point has to be the value of communication data both to the police and to the intelligence agencies. The police evidence is very clear. It has

huge importance in ordinary crime as well as in countering terrorism and cybercrime. From that starting point, we have to have an authorisation process that can cope with the number of requests, which is over 500,000 a year, so talking about requiring warrants to be signed by Secretaries of State or senior judges is not appropriate. The justification for that was that it is less intrusive to look at communication data than to look at content, and that principle is reflected in the Bill.

The point I was making to the Science and Technology Committee is that there will be some hard cases, and Professor Anderson gave some examples of precisely that. If you move the cursor too far over to be so restrictive, you create a real problem about the authorisation of data communication requests. If you move it too far the other way, you get the equal and opposite problem of not sufficient authority being applied. The cursor is more or less in the right position, because it has taken the RIPA 2000 definition of who called whom, where and what, and transferred it to the computerised age of which device contacted which server up to the first slash of the address, but there will be hard cases. I was suggesting to the Committee that you have to be pragmatic and ask whether the overall public interest in the authorities and police having this information, which is vital for upholding the law and bringing people to justice, balances the fact that you may occasionally have a hard case. In my view it certainly does.

Baroness Browning: If we get the definition right and if we get the clarity that the panel seems to feel is lacking at the moment, do you think that will serve us for now, or will we have to keep revisiting this?

Professor Sir David Omand: For the sake of clarity, I think the definitions are clear; it is reality that is fuzzy. The parliamentary draftsman has done a very good job trying to clarify this. I am not sure you can make it any clearer.

Baroness Browning: That is very clear. Thank you.

Dr Paul Bernal: This is a really important element. Sir David said that communications data was less intrusive than content. I do not think that is true. They are differently intrusive. There are several reasons communications data can be more intrusive. One is that it is by its very nature more suitable for analysis and aggregation. You can do more processes to it than you can to content. That means that it is subjected to what we loosely called big data analysis. It is also less hard to disguise in some ways. You can talk about a coded, not encrypted, message to somebody. In England we do this all the time; when we say “quite”, it could mean a million different things depending on the context. You cannot do that so easily with communications data. That means that sometimes you can get more information out of communications data than you can from content. I do not think you should be under any illusions that somehow it is okay to have as much communications data gathered as possible but not okay to get content. They are different things. For individuals, sometimes content matters more; en masse, communications data matters more.

The Chairman: Before you came in we were discussing the differences between communications data and content, but the drafters of the Bill and the Government who sponsored it seemed to indicate that there is a significant difference in terms of people’s

privacy with regard to what is written by them and to them, as opposed to the hows, the wheres and the whens, but you are contesting that.

Dr Paul Bernal: I am contesting that. I would say that it can be worse. You have at least some control over what you write, whereas for communications data largely you have very little control over it at all. It is a different sort of intrusion.

Q88 **Baroness Browning:** From the point of view of the speed at which things change, could you indicate whether you think that even if we had an imperfect definition, in your terms, we are going to have to keep coming back to legislation more quickly to update it? Is that a danger?

Dr Paul Bernal: Frankly, yes.

Baroness Browning: Do you think we will keep coming back to this?

Dr Paul Bernal: I think you will be coming back to this and you should be, because things change in so many different ways. This is not the sort of law that you can set down and say it will last for 15 or 20 years without amendment, because the technology is moving too fast; people's behaviour is changing too fast.

Baroness Browning: May I bring you back to Sir David's point? Seeking perfection is perhaps something that we should compromise with pragmatism.

Dr Paul Bernal: You should, but you should compromise it by adding extra oversight rather than by accepting a loose definition, by making sure you can monitor what the intelligence and security services and the police are doing so that pattern of behaviour matches the intent behind the law as well as the definition. This is part of Lord Strasburger's analysis of how powers have grown without parliamentary approval. It is very easy and we have seen it historically again and again. People have not been watching what is going on and you need to continue to monitor things. I am not yet convinced that the oversight arrangements here are strong enough to do that. The idea of, if not a sunset clause, a revisiting clause of some kind might be worthwhile, and also monitoring the monitors: how are the oversight arrangements working?

Q89 **Stuart C McDonald:** Turning to communication service providers and the requirement that could be placed on them to store up to 12 months' worth of communications data and Internet connection records, how feasible is it for providers to do that?

Professor Ross Anderson: It could be extraordinarily difficult and expensive if they are to do what they are advertised to do. We are told that Internet connection records will enable the agencies and police to get past what is called carrier-grade NAT, which is a technique whereby the IP address of your mobile phone might be shared with 1,000 other mobile phones, the idea being that, if someone does a bad thing online on Monday, you ask O2 and they say that it could be any one of 1,000 phone numbers, and, if the person does another bad thing on Wednesday, you have another list of 1,000 phone numbers and you say, "Aha! The common number on the two lists is this one". It is not going to work that well, first because you will find hundreds of common numbers on the list; and, secondly, if you want to relate that to things people have done on other service providers, you have to

relate it to an ID on Google, a handle on Twitter or a logon for Facebook. For that, you would have to require the communication service providers to store very much more data than they do at present. You would have to get them to store precise time stamps, addresses and so forth, which they will not do.

ICRs will not work as advertised. What they will do is create an extraordinary capability power for investigators to say, "Show us all the websites that these two bad people have visited in the past month and all the other people who have visited the same websites". If you want that capability, which appears to be what is intended, you end up requiring lots of people to store lots of stuff. There is, first, the issue of cost if you are to remunerate communication service providers in Britain; and, secondly, there is the likelihood that service providers overseas will refuse outright because it would be too much effort and energy to redevelop their systems, and Britain is only 4% of the market anyway.

Dr Paul Bernal: The Danes are the people who have got closest to doing this, and I would recommend, if you can, to get one of the witnesses from the Danish abandoned attempt. They ran it for nearly seven years and got almost no useful information out of it, but there was a huge cost, even though they were warned beforehand by the ISPs, as I believe they will be here, that this is not a practical proposition and is not likely to be an effective one.

Professor Sir David Omand: The Committee will discover, if they do that research—I hope they will—that the model the Danes chose is not the model I strongly suspect the Home Office would choose. The Danes themselves are revisiting it at this very minute because they may find post-Paris that it is necessary to go back and look at it.

Q90 **Matt Warman:** I want to talk a little about encryption or decryption. Do you think it is reasonable for Government even to ask communications providers to provide unencrypted material for something that is currently encrypted?

Professor Ross Anderson: There is a power in Section 3 of the RIP Act which allows them to do that. As I remarked earlier, Parliament saw fit to hedge it with very stringent safeguards. Nowadays, it would be much more difficult, because many service providers encrypt stuff by default. They do so not out of any particular malice towards agencies but simply to stop other people stealing their ads and customers. It has just become the commercial default; it is what everybody expects. With messaging services, everybody increasingly expects stuff to be encrypted end to end. The Government of Kazakhstan have recently decreed that everybody has to install the Kazakhstan Government's cert on their machine from 1 January. I predict that if you have an iPhone in Kazakhstan you will suddenly find that none of the services works. That will be worth watching.

Matt Warman: Sir David, do you have any thoughts on whether we are likely to get anything meaningful out of demanding unencrypted data from people who currently encrypt it anyway?

Professor Sir David Omand: Of course, you will be distinguishing between content data and communications data, which clearly has to be delivered in a form in which the authorities can use it. If we are looking at content data, as far as I can see there is no back-door encryption provision in the Bill. The Government have said that they are not seeking it. I know the agencies are not seeking it, so as end-to-end encryption spreads it will get harder

and harder for the authorities to be able to access unencrypted content, even for their highest priority suspects. That is a fact of life.

Does that mean that the authorities should have no power to seek such information, and to do their best in cases where it might be available? That is the approach I would commend to the Committee. It is a power to seek, but I do not think it is in Parliament's power to insist that all encryption can be bypassed, nor would it be a very sensible thing to ask for in terms of the national economy and the need for the Internet to be secure. There will be specific cases where it will make sense and information could be made available, and the Bill should provide for that.

Matt Warman: To be clear, in general you do not see the Bill as providing the back door that people have spoken about.

Professor Sir David Omand: No, I do not.

Dr Paul Bernal: Many of the companies concerned do not share Sir David's view, and that is one of the reasons why some of them are distinctly disturbed by news of the Bill. One other thing that we need to be very clear about—Professor Anderson has already referred to it—is that we do not want to put British companies at a disadvantage, because they are more likely to be subject to the force of British law than a company in California or Korea. If we put the power in place to allow them to do it, they are disadvantaged, and that is not good for anybody.

Matt Warman: Which only emphasises the need for clarity, does it not?

Dr Paul Bernal: Clarity is what is needed.

Q91 **Matt Warman:** To move on to equipment interference, what does the panel understand that to be?

Professor Ross Anderson: It is basically hacking or the installation of malware, or what the NSA calls implants and what we call remote administration tools in a machine. If I am a bad person, the police would be able to say to O2, "Put an update on the android on Professor Anderson's phone", and that would enable them remotely to turn it on, use it as a microphone or room bug, or look at me through the camera, collect my location history and all the rest of it. What is more, as we get digital stuff in more and more devices they could do the same to my granddaughter's Barbie doll; they could do the same to your car or your electricity meter. It is open season on the Internet of things. It goes without saying that the controls around that need to be very carefully drawn; otherwise, it undermines trust. If UK producers of stuff can have their arms twisted to provide a capability to put implants into stuff, why should people buy stuff from Britain?

Professor Sir David Omand: I agree with the point Professor Anderson makes about the need for careful oversight of this, but the power already exists; it is already in use under existing statutes, including the 1994 Act. It is of inestimable value to the intelligence agencies, particularly on national security addressed to targets overseas where there are

legitimate demands for intelligence. Some 20% of GCHQ's output benefits from that kind of technique. There is nothing very new about it.

Dr Paul Bernal: There is nothing new about it, but there is something new about our behaviour and the technology we all use. Twenty years ago I was not using anything that was encrypted at all; now half the stuff I have on my phone is encrypted by default, and another batch is encrypted by choice by me, so for normal people this now becomes relevant when it was not relevant before.

Professor Ross Anderson: What is new is that we found out about it thanks to Edward Snowden, and GCHQ admitted that it was doing it just in the last month or two, thanks to the case currently before the Investigatory Powers Tribunal. People are beginning to get worried about it, and with due cause.

Q92 **Lord Strasburger:** Gentlemen, can you help me out with bulk personal datasets? The Bill and the Explanatory Notes are very vague about that. The ISC report was rather vague about it—it was hugely redacted. The Home Office will not tell the Committee the identity of the databases it is scooping up, so it is very difficult for this Committee to assess the proportionality, risks and intrusiveness of the collection of bulk personal datasets. Does anybody know what they contain? Do they contain medical records? Do they contain bank records? What do they contain?

Professor Ross Anderson: For starters, we know that the police have access to things like credit reference and DVLA records. That is public knowledge. Secondly, they have access to medical stuff. They have had that since 1996. At the time, I happened to be advising the BMA on safety and privacy and that sort of thing came through. Thirdly, in any case, hospital medical records were sold on a wide scale in the care.data scandal last year, and it would have been rather negligent if GCHQ had not grabbed a copy on its way past. Fourthly, it is well known that some kinds of bank records, in particular all international financial transactions, are harvested on their way through the SWIFT system.

Professor Sir David Omand: Not true.

Professor Ross Anderson: This has been a matter of enormous contention in the EU and elsewhere. It is only to be expected. If I were, for example, an investigator for the FCA, I would want everybody's bank statements too.

Professor Sir David Omand: Chairman, it is important not to allow fantasy to intrude at this point. The central bank governors responsible for the SWIFT system agreed that that system could be searched for specific transactions of known criminals and terrorists. That is public knowledge. All SWIFT data is not scooped up.

Lord Strasburger: Perhaps we could impress on the Home Office the need for the identity of these databases to be revealed.

The Chairman: That is something that we would have to do in private session, but I take the point that there is a serious difference of view between the witnesses on what is a hugely important subject.

Q93 **Dr Andrew Murrison:** I am going to be fairly brief, because I think we have covered quite a lot of this already. I refer to the international dimension. We sit here thinking we can make various laws and regulations, but we are talking about a global industry. Referring to some of your previous comments, could you reiterate the likely reaction of the international community to the Bill, in particular the feasibility of gathering ICRs, given that it is entirely in the gift of companies whose headquarters are not in the UK?

Professor Sir David Omand: We took evidence on this as part of the independent surveillance and privacy review run by RUSI and we got a variety of answers from international and British companies. Some of the companies said that as a matter of corporate social responsibility they wanted to be in a position to provide this kind of information for the purpose of preventing serious crime and terrorism, but they felt extremely nervous about doing it without a firm legal basis on which warrants or authorisations would be made. Other companies said that as a matter of company policy they did not believe their data should be made available to any state or law enforcement authority. You have a variety of views. The provisions of the Bill, which include the provision that the Home Secretary can make judgments about what it is reasonable to expect, will be partially successful; but they will not be completely successful, because some companies will simply refuse, and I cannot see the British Government attempting to launch civil actions against major players.

Dr Andrew Murrison: Presumably that means that the disinclined would note those who were complying and those who were not and go for those who were not.

Professor Sir David Omand: The intention is not to make public the companies that comply and those that do not.

Professor Ross Anderson: We all know the companies that will comply. They are the ones that get large amounts of their revenue from Governments, or that rely on Governments for capture regulators—companies such as IBM, BT and those set up several generations ago. Companies that have been set up in the past 20 years think differently because they have a different culture—the Silicon Valley culture. Their money comes either from their users directly or from advertising—from their users buying stuff or being advertised to—and they take a completely different view. It is not much good getting BT on board if all BT is doing is providing a piece of copper wire from people's houses to where the real action starts, so it is the view of the big American service companies that matters more than most. They are going to drag their heels.

There is the issue of foreign Governments. There is also the issue of what happens to small start-ups in the UK, which is absolutely crucial. For example, about five years ago one of my postdocs set up a security start-up. Because of the arm-twisting that the agencies have always indulged in, he decided to set up a coding shop in Brno in the Czech Republic. More and more people will be doing that, simply as a matter of default. You cannot run a tech start-up nowadays unless you have a marketing operation in North America, because that is where you make your first sale and most of your initial sales. If we create a regulatory regime where it is only common sense for people to put their coding shop, their

engineering, in North America, Seoul, Mumbai or wherever, the cost to us directly or indirectly down the stream of time will be huge.

Dr Paul Bernal: We have to be aware of where things are moving. There may be a number that are co-operating willingly now, but that will shrink. More and more companies are likely to say, "No, we are not going to give this", and they will be the bigger and more successful ones. You make yourself a hostage to fortune by assuming that this will end up functioning.

The Chairman: Thank you very much indeed. I thought the whole session was absolutely riveting. You have given us an enormous amount to think about. Obviously, you have very different and varying views on the issues before us, but you highlighted issues that very much need highlighting. I know that members of the Committee are grateful to all four of you for giving us your very robust and significant views on this important Bill. If you would like to add any written evidence to supplement what you have said, we would be more than happy—indeed delighted—to receive it. Thank you very much indeed.

Renate Samson, Chief Executive, Big Brother Watch (QQ 127-136)

Evidence heard in public Questions 127-136

Oral Evidence

Taken before the Joint Committee

on Wednesday 9 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Lord Henley, Lord Strasburger.

Witness: **Renate Samson**, Chief Executive, Big Brother Watch, gave evidence.

Q127 The Chairman: A very good afternoon to you—or evening, now. I am sorry that we are a little late—there was a vote in the Commons earlier. You are very welcome. I will make two points before I ask the first couple of questions. My colleagues will come in after that. Each of you has given your response to the Bill very publicly over the last number of weeks. The Committee has all the statements that you have made. In addition, of course, I am sure that you will give us written evidence. This is a very big Bill. It is very lengthy and very technical. Has subsequent analysis of the draft Bill led any of you to alter any of your positions from those that were taken in your initial response to the Bill's publication?

Shami Chakrabarti: I would simply say that I am possibly more alarmed by the Bill than I was at first glance. The Committee will appreciate that it is a long Bill.

The Chairman: Very long.

Shami Chakrabarti: It is very complex. Like all legislation, it requires an understanding of what its clauses actually provide, as opposed to how its clauses have been pre-briefed or spun in the press. It also requires a level of understanding of the relevant technology. Those two things have to come together. My own organisation is a human rights organisation with, traditionally, considerable expertise in legislation, but recent weeks have given us the opportunity to work with partner organisations that have a considerable level of expertise in the technical sphere. That experience makes me more alarmed now about the personal and cybersecurity implications of the provisions, however laudable and well-meaning they may be in their motivation.

The Chairman: Do your colleagues share that view? Are you more alarmed now, as the weeks go by?

Renate Samson: Initially I was very clear that there was a lot to read. I have now read through it. The implication was that there was a lot of transparency. At first, it seemed that that was the case, but, as you read more and more, you find that there are a lot of vague terms in the Bill that require a lot of head-scratching to try to understand exactly what may be meant. Trying to engage the public in understanding what the Bill says and what its

implications for them will be has been a challenge. There probably need to be many more readings of the Bill before you can get to the bottom of even a tip of what might have been meant.

Caroline Wilson Palow: I agree. We did and do welcome the opportunity to engage in this process. As we have started to get into the Bill, which is long and complex, we have started to notice a few things. For instance, Part 6 is about bulk powers, but when you look into some of the other particularly targeted provisions, you start to see that aspects of those look quite a lot like bulk powers in and of themselves. The service provider provisions that are sprinkled throughout the Bill put a lot of obligations on service providers, which I know you have often heard about, and which seem like they could undermine both security and trust. Those were not things that were necessarily apparent when we first took a look at the Bill. Another particular provision that concerns us a bit is Clause 188, on national security notices, and how that will play out in conjunction with the other provisions of the Bill.

Jim Killock: We have been particularly alarmed by the reintroduction of the so-called filter, which complements the collection of very widely defined Internet connection records. The filter seems to us to be essentially a federated database and search system, very much like previous incarnations of the Communications Data Bill, the snoopers' charter or the intercept modernisation programme. It has been proposed a number of times and stopped a number of times, because of the power to look into people's lives that it would give. In a sense, that deserves an entire debate on its own, as does the recent admission of collection and use of bulk datasets.

What is a bulk dataset? Which of them have been accessed and grabbed by GCHQ so far? To whom might that apply? Just about every business in the country operates a database with personal information in it. It could be Tesco Clubcard information. It could be Experian's data about people's financial transactions. It could be banking details. It could certainly be any government database that you care to mention. From that perspective, it is hard to see where surveillance ends as a result of bulk datasets. Traditionally, we have thought of surveillance as being about communications data and as being targeted. In this Bill, we have various measures for blanket collection—bulk collection, as it is referred to—and we extend that to any private or public institution that happens to have data. From that perspective, it is pretty worrying. It is hard to see the start and end of it.

One good thing that we did not necessarily expect is that there is a thorough or, at least, a large document spelling out the apparent operational case for Internet connection records. The fact that that has been produced is a welcome step. A very important thing to do when asking for a new power is to produce documentation explaining why it might be needed. That said, it again requires examination on its own behalf, as do the GCHQ powers. They need an operational case. Parliament has not debated why GCHQ has those powers; it has merely been presented as something that is happening and that we should now legitimise. In the USA, those kinds of powers were examined—bulk data collection and use under Section 215 of the Patriot Act. An operational case was made and was reviewed by bodies that were trusted by the President and by the USA's democratic institutions—the Privacy and Civil Liberties Oversight Board and the NSA review board. Both came back and said that there was no operational case for the bulk collection and use of data; nothing the NSA had done showed that that data had prevented anything significant. That kind of review needs

to happen here. The fact that it has happened in the USA and they have come up with the conclusion that these programmes need rolling back ought to be something that you consider carefully. Parliament really needs to examine those operational cases.

Q128 The Chairman: I think that I have got the message. I am assuming that you do not think that the Bill strikes the right balance between security and privacy. Without going into detail—my colleagues will ask questions on different parts of the legislation—other than dumping it altogether, do you think that it could be improved?

Shami Chakrabarti: It could certainly be improved. One thing we would all agree on, and would agree with the Government on, is that there needed to be a new Bill, in the light of Mr Snowden's breathtaking revelations. Whether you consider him a hero or a traitor, there is no doubt that he revealed practices and capabilities where we, the people of great democracies on both sides of the Atlantic and all over the world—I would include parliamentarians in that definition of the people—had little or no idea of the sheer scale of mass surveillance that was being conducted against populations. There is a debate to be had, of course, about how much of that should or should not happen, on what basis and with what safeguards, but in the light of that there had to be new legislation, because whatever was happening was happening, at best, on very creative interpretations of outmoded laws. Some of us would suggest that it was happening outside the law and without sufficient parliamentary scrutiny, public discourse and legal authority.

We certainly agree that there must be a new Bill; there must be something like this Bill. My fundamental objection is that too much of it is about sanctioning mass surveillance of entire populations and departing from traditional democratic norms of targeted, suspicion-based surveillance, for limited purposes. There are insufficient safeguards against abuse. For example, there is the argument that I know you have had extensively about the role of the judiciary. Our position is clear. This is not a system of judicial warrantry. This is Secretary of State warrantry, save in one of the most chilling provisions of the Bill, which is about hacking and the new concept in public understanding of what the authorities propose to do. We think that is one of the gravest powers, because potentially it leaves long-term damage to systems, individuals, devices and security, after a perhaps justifiable investigation. That has the lowest safeguard of all, because in certain circumstances it involves not even the Secretary of State but, for example, a chief constable. There is too much surveillance, there are too many people, it is not to a tight enough threshold or a high enough standard and there is insufficient authorisation by the independent judiciary.

Caroline Wilson Palow: Following on from that and your introduction to the question, security and privacy are not necessarily mutually exclusive. The hacking provision, in particular, shows that there is a lot of potential to undermine security by allowing that power, including the fact that the use of malware—the type of software that allows access to computers through hacking—is not necessarily well controlled. It is like breaking a lock on a door and leaving the lock broken, so that other people can potentially get in and access the same device or equipment that was targeted in the first place. That is an example, within equipment interference, of some of the security problems. There are also greater, overarching concerns about undermining things like encryption standards and whether or not that would be permissible, both under the hacking provision and under some of the provisions, like Clause 189, which say specifically that the removal of electronic protection could be required of service providers that are subject to compliance with warrants and

authorisations under the Bill. Finally, data retention in and of itself has certain security concerns. Of course, as we have recently seen with TalkTalk here or even the Office of Personnel Management in the US, there are breaches. When you are mandating companies or even Governments to keep more information, it makes the breach even worse when it happens.

Renate Samson: I support the points that have been made about concerns with regard to safeguards. Caroline made the point that privacy and security are two sides of the same coin. We also have to look at the idea of protection. Part of this Bill is about protecting the public, yet, as has been pointed out, there are other elements that will potentially make the public vulnerable, whether that is through equipment interference or through weakening of encryption, for example. We have to step back and have a think about what protections the public require with regard to the proposals in the Bill. The idea of full independent judicial authorisation is something that I know you have been discussing at length. I would support the view that it needs to be explored in a lot of detail. We are on the cusp of being complete digital citizens. We do not have a choice any longer about our engagement online. Proposals that suggest that online engagement can be surveilled at any time, potentially, and retained for a number of months are a worry to us all. It is not the case that the Bill should be scrapped, but there are certainly areas that need to be strengthened greatly.

Suella Fernandes: On the flipside of those comments, do you equally accept that the scale and nature of the threat that we currently face is unprecedented and severe?

Shami Chakrabarti: I do not doubt that the world faces enormous threats from crime, terrorism and so on. I do not think that any of us doubts that. The question is how best to counter those threats. I will repeat the previous remarks, which are really important. It is not about a trade-off between privacy and security. A lot of what we are concerned about is actually security. What is national security if not the personal and, increasingly, the personal cybersecurity in relation to where I am—whether somebody is in my house, engaging online, and whether I am away and, therefore, open to an attack or a burglary? My financial records and so on are part of my personal security and cybersecurity. National security is to some extent the combined personal and cybersecurity of millions of people. We think that up to 50 billion emails are intercepted every day by UK authorities. There are only 7 billion people in the world, and only 3 billion of them currently have access to this kind of technology. To me, that in itself is a threat to personal security—not because the authorities are malign, but because when you collect data and create vulnerabilities, that data can be attacked by non-governmental sources and the vulnerabilities that have been created can be attacked similarly.

Suella Fernandes: On the vulnerabilities you talk about, you point out the scale of, for example, communications data and equipment interference and interception, but those powers have been absolutely essential and critical to successful convictions for large-scale child sexual exploitation, human trafficking and serious and organised fraud and crime. Those are powers that are currently exercisable by our law enforcement services. The Bill represents a drawing together and consolidation of existing powers.

Jim Killock: We are talking about several different things here. There are policing powers, there are data retention powers and there is extension of those for the police in the ICRs and the filter, so you have that body. Then you have the other area around GCHQ—what it does and how it gathers information. You have to look at both of those quite separately.

You are really asking about the operational case. As I said, my problem with the operational case is that it has not been presented to anybody for GCHQ. When the equivalent was done in the USA, the President of the USA and its democratic institutions decided that there was not really a case for a lot of it and decided to roll it back, because it was essentially purposeless. Here we have an operational case for the police with regard to ICRs, but we do not have the mechanisms, because we do not have a civil liberties board in the UK. It has not been constituted, despite potentially being put into law. That has not been examined.

On data retention in general, we have had a ratcheting back of data retention in a lot of Europe. These apparently essential tools have not been operational for a long time in Germany, the Czech Republic, Slovakia and a number of other places. There are about six or seven countries where these sorts of programmes have essentially been cancelled. There has not been a concomitant outcry from the police that they are no longer able to solve crimes and that there is spiralling dysfunction in the police. That has not occurred. Something to bear in mind is that there are often several routes to solving crimes. Data, through data retention or collection, is only one. That data probably resides on laptops and mobile phones. It will reside at service providers. That is talking only about the data side of it; there will be other kinds of factors in the equation. It would be interesting to hear from Caroline about data preservation and the standards elsewhere.

Caroline Wilson Palow: The US, for instance, does not have a data retention provision, yet it is still able to solve crimes. In fact, it uses mechanisms like data preservation orders, which are much more targeted, are not across the board and can be quite effective. You also have instances, which have been mentioned, of places like Germany, the Czech Republic and other countries in Europe where data retention is either much more circumscribed or non-existent. Again, we have not seen a collapse due to the fact that it is not there.

To pick up another point you asked about—the existing powers, particularly in the context of equipment interference—it is true that it was revealed earlier this year that the intelligence services were engaging in hacking and, when this Bill was introduced, that law enforcement, too, was engaged in hacking. Until that point, that had not been revealed publicly. The reliance on the Intelligence Services Act and the Police Act, which are incredibly broad powers, to say that that was already in statute is inappropriate, because they are so broad. There was no indication that it was actually happening. Since those Acts are from 1994 and 1997, if there was an indication in the Acts that hacking was possible, why was there concern not to reveal it sooner? Why was the position of the Government until earlier this year neither to confirm nor to deny that those powers were being used? While they may have been in use, they have not actually been in law up to this point. That is why we talk about them as new powers in this Bill.

Shami Chakrabarti: I have one further small point on comparative practice around the world and the importance of law enforcement. There is still no provision for intercept

evidence to be admissible in criminal proceedings. There has been and is to be all this interception, for laudable criminal justice purposes—public protection and law enforcement—but there is still not the provision, for which some of us have asked for many years, for interception, when it is proportionately and lawfully gained, to be used in criminal prosecutions, as is the case all over the democratic world and among our allies.

The Chairman: Thank you. I move to Dr Murrison.

Q129 Dr Andrew Murrison: I am getting the sense that you are not convinced that the "double-lock" provision, about which much has been spoken in recent weeks and on which much store has been put by those who have been involved in bringing the Bill to the position it is currently at, is really much cop. However, I believe that it is likely to remain a feature. Given that it is likely, what do you think could be done to improve the double lock? Would you see virtue, for example, in distinguishing national security from serious crime, having the double lock apply to national security and having judicial authorisation only for serious crime? Would you see virtue in, for example, a different means of appointing the information commissioners who will be involved in this process?

Shami Chakrabarti: Some of my colleagues are the great technologists and experts. I am just a humble lawyer in recovery—or in remission—so I find it easier to make the analogy with the real world when I am dealing with the virtual one. We are digital citizens, but we are still people and citizens. If I want to search your house or your office for laudable reasons, I go to a magistrate for a warrant. I can understand the argument coming from the Government that when we are doing this national security stuff and, perhaps, spying on foreign Governments, we cannot just go to any old magistrate. There has to be a double lock, surely, on something as serious as interfering with the German Chancellor's communications. That is such a political decision that there ought to be some Executive involvement. The double lock is simple: have a provision across the board for judicial warrantry, but as an internal administrative matter, make sure that those warrants are not sought by the authorities unless they have been to the Home Secretary first. In the non-crime cases—the international relations/national security cases—as a matter of good public administration, go to a Secretary of State first, but always have the sign-off to protect people's rights and freedoms, whether in the UK or around the world. Have that sign-off by a judge, as you would for your home, your flat or your office. Again, that is the practice across the democratic world.

Renate Samson: I second that. A large part of what we find ourselves doing when it comes to the digital world is incomprehensible to most of us, because it is invisible, yet we all understand what happens when somebody knocks at our door and asks to have a look around because they suspect us of something, and that element of being suspected of something is important. The real world understands a judge signing off on something. The general public have confidence that there is independence to it. While we may currently have a benign Government, we do not know what the future holds. This piece of legislation should hold up for many years. We do not know what the future will bring, so independence is hugely important. That will also mean how the judges are appointed. To feel genuinely that surveillance conducted upon us is being assessed independently and with no interference from anywhere else will reassure the general public that, should the

rest of the provisions in the Bill become law, they will be secure and thoroughly thought through, not just signed off with a flick of a Minister's pen.

The Chairman: It is said that a Secretary of State is ultimately accountable to Parliament for his or her actions, whereas a judge is not. What is your view on that?

Renate Samson: You took evidence at the beginning of this week from Mr Paterson and Lord Blunkett. I think that they answered that question for you, in that neither of them has ever stood up in Parliament and talked about a warrant they have been involved in signing off.

Jim Killock: It is also worth reminding ourselves how we got here, in a sense. The Regulation of Investigatory Powers Act had powers for the collection of material from persons overseas. The meaning of that warrantry system was extended through practice to mean every communication passing between the UK and the USA. That is how the Tempora system of bulk collection was created—through those warrants, which were politically authorised. There was a political decision, alone, to extend the meaning of those RIPA warrants, which meant that essentially Parliament was cut out of the decision, right or wrong, to engage in the programmes of bulk collection of data that we are now authorising in this Bill. It seems to me that if one is to restrain the Executive from creative interpretations of the statutes, as Shami said, you need that judicial authorisation. They should be saying, "Minister, I do not think that this is necessarily how the system was designed to work. Perhaps you might like to consult Parliament". That is a far more likely outcome than the Home Secretary saying to GCHQ, "No, I am going to deny you those powers for one or two years while I work out a political opportunity to legislate".

Caroline Wilson Palow: In conjunction with that point, it means that the judicial commissioners need the full ability to assess the warrants when they come to them. It should not be just a judicial review standard. They need to assess fully the substance of the warrant and, among other things, whether there are other less obtrusive means by which this information could be obtained. That is an easy edit to the Bill. Every time the judicial review provisions appear—it is at subsection (2) of most of those clauses—you just delete it. You take it out.

Suella Fernandes: Are you saying that the double lock and the judicial involvement strike the right balance in having judicial review as an element of the decision-making process, or are you saying that it should not be there?

Shami Chakrabarti: Judicial review does not help at all in this context. When you are deciding whether it is proportionate to issue a warrant for intrusive surveillance of an individual, let alone of a whole group of people, that is a judgment made on the evidence. A judicial review test only second-guesses the Secretary of State, in very limited circumstances. Did they make a bonkers decision that no reasonable Secretary of State could take? That is not judicial warrantry. In the statute there should be a one-stage test: the judge signs the warrant. However, because people are concerned about cases of interception on foreign powers, for example, which is classically a matter for the Executive rather than for independent judges, police officers or whatever, interception and so on of foreign statesmen and powers should go to the Home Secretary first, as a matter of good

public administration. You would not even need that in the statute, or you could put it in the statute for that category of case.

Renate Samson: Your question is interesting. I have listened to a number of the sessions of evidence that you have taken. You have all posed the question a number of times, "What exactly is meant by judicial review?". Witnesses have given you a variety of versions of what judicial review means. There is lack of clarity.

Suella Fernandes: That is exactly what I was going to raise in my question. You will agree that, with judicial review, the judge would have access to the same information as the Secretary of State or the Minister.

Shami Chakrabarti: I do not think that is suggested in the Bill. There is nothing to suggest that.

Suella Fernandes: That is what judicial review involves, does it not?

Shami Chakrabarti: No, it does not. This is a term of art. A judicial review test, as a matter of our law, is a very limited opportunity for a judge to second-guess a decision that has been made by a public authority, whether it is a Secretary of State, local government or whatever. It is not a double lock.

Jim Killock: Basically, it is, "How did you follow procedure?", is it not?

Shami Chakrabarti: Yes. Did you make a decision that was within the realms of a reasonable decision? Could any reasonable Secretary of State possibly have made that decision? It is not appropriate for warrantry.

Suella Fernandes: What about the proportionality test, which involves balancing the right infringed and the objective met? That goes further than what you are suggesting, does it not?

Shami Chakrabarti: But that has not been allowed to the judge, under the provisions of the Bill. They are not second-guessing the Home Secretary's decision on the merits of proportionality, under the Bill.

Caroline Wilson Palow: That is exactly our concern. When you talk about judicial review, all you are doing is looking to see whether proportionality has been assessed by the Secretary of State. The judge will not have the power to say, "You have made that assessment incorrectly". In the US, to give an example of a comparison between two different types of warrantry there, a normal warrant would go directly to the judge. There is a political consideration that is made ahead of time. For instance, the US attorneys, who are the federal attorneys who often start the process, are politically appointed and will make a decision about whether or not to seek a warrant in the first place. Once that is done, it goes directly to the judge.

Suella Fernandes: Before we finish this line of questioning—I know that other people want to get in—I need to put on the record that the statute states explicitly that it must be "proportionate" and "necessary". That is the relevant test.

Shami Chakrabarti: You have to look at Clause 19(2).

Caroline Wilson Palow: The concern is the way in which the two play together. That is why I said that we think you should just delete subsection (2). We totally agree that necessity and proportionality need to be assessed, but, once subsection (2) is in there, it reduces the ability of the judicial commissioners to make that assessment. To continue the parallel that I was trying to draw, in the US there has been a lot of talk about the FIS Court, which acts on foreign intelligence. This is PRISM—the types of authorisations for collecting intelligence on people around the world. Its powers are the equivalent of what judicial review would be here. Essentially, when a request comes to it, it has to check the box to say that everything has been considered as necessary, but it does not necessarily get to question the conclusions that were reached by the person who was seeking the warrant in the first place.

Shami Chakrabarti: A double lock would mean, "I can substitute my decision on the merits for yours". Traditional judicial review means, "I look at the way you made your decision, but I do not substitute my own for yours". You have to be procedurally irregular or to have made a completely insane decision that no Secretary of State could make. That is achieved by Clause 19(2), otherwise there would be no purpose to it.

Matt Warman: We have had an awful lot of witnesses tell us that their expectation and understanding of what the Bill says regarding judicial review would, as Suella Fernandes has said, in fact mean a test that looked at the evidence. It would have to be proportionate and go through all those things. You are saying simply that that is not your understanding of judicial review. It therefore seems to me that we are talking simply about definitions; we are not actually talking about a principle, because what we have been told is what you are saying you are asking for.

Shami Chakrabarti: It just does not stand up in law. These are well-tested terms. If you want to create a full merits appeal in statute, there are many precedents for doing that. You do not put in a clause like 19(2); you can do it much more simply. I believe that you will hear from the Secretary of State in the not-too-distant future. You can just ask her: "Is it your view that you will make an initial decision and there will be a full merits review? The judge can just second-guess your decision and make a different one. Is that your intention?". If she says that that is her intention, that will help for Pepper v Hart purposes, but there are far clearer ways to deal with it, like just deleting Clause 19(2).

The Chairman: Thank you. Can I move to Mr McDonald?

Q130 Stuart C McDonald: I have another million-dollar question. What is your understanding of the meaning of the term "Internet connection record"? Why would their gathering and analysis be more intrusive than for other forms of communications data?

Shami Chakrabarti: This has been quite a journey for me. I have had lots of younger and more technologically savvy colleagues explain the sheer scale of what we might be looking at as regards Internet connection records. If you take your favourite device—your smartphone, your tablet or just the sites you go to from your laptop or desktop—we are looking at things like the websites you visit. We are looking at the communications software that you might use to speak to your mother—Skype, WhatsApp and so on. We are looking at all the icons on your menu, such as your Twitter and your diary. Recently a health one popped up on my phone uninvited, telling me how many steps I took yesterday. Taxis,

maps; the list goes on. Photos, my Internet shopping, banking apps—I understand that all those things are potentially within the broad concept of Internet connection records. As we look just a little way into the future, in the discussion that people describe of the Internet of things, more and more of our real lives will be managed online. Now we will be talking more and more about the little icons on our devices that connect to our fridges, our cars, our burglar alarms, our gaming devices and so on, so the separation between my real-world security and privacy and my cybersecurity and privacy is almost completely collapsed. This is very intrusive on millions and millions of, for the most part, completely innocent people.

Renate Samson: It comes back to the point that I made that we are all now digital citizens. It is that—it is life. It may feel at the moment that it is just a mobile phone and a laptop, but, as Shami explained, with the Internet of things it will be everything. That will create a huge amount of data that will be constantly ticking over. We have been informed that the Internet connection records are just the URL, before the first slash, of a website and no content, but from the technical evidence I have been listening to and you have been receiving, and from all the different things that I have read, which Jim will probably be able to explain better, I am not entirely sure that it is quite as clear-cut as has been implied. I would certainly like to hear from the Home Office—from government—with regard to this Bill a very clear definition that it knows exactly how this can be done, because I am not sure that I do.

Jim Killock: It seems to me that essentially the Internet connection record starts from the point of view that the Home Office wants the power to have retained the fact of somebody using the Internet, with some other service, and to record that. It has decided that the best way to do that, given how much the Internet is used, the purposes it might be put to in the future and the services that might appear, is just to say, "Let's have a very broad definition of anything that connects to anything, whether it is a person or a machine. That will allow us to compel Internet service providers to collect information about anything we deem important in the future".

I do not think that is really a good way to legislate. It is incredibly broad, it is open to abuse and the cost implications are impossible to put a number on. If you have power to collect and retain any information, no matter how difficult that is and how much of it there is, essentially you have just written a blank cheque to scale up surveillance indefinitely. Of course, once you have an initial investment and the thing has started to roll out, that poses the problem of how you restrain it in the future when it turns out to be not quite as useful as you hoped. Do you pour in another few tens of millions of pounds to extend the amount of information that you are collecting under this very broad power? Given that the companies will probably tell the Government that it will be more effective if they spend that extra bit of money, this seems to be a financially haphazard way of working, as well as haphazard in terms of human rights and the proportionality of the surveillance we are authorising.

Caroline Wilson Palow: This is quite a confusing definition, because essentially you have two different definitions in the Bill. You have Part 3, where Internet connection records are explicitly mentioned, but in Part 4, under data retention, you have a clause that, under the commentary, is supposed also to encompass Internet connection records. The definitions

do not completely align, and for that reason we are somewhat confused about what Internet connection records really are.

Let us take an example from the commentary that Renate has already mentioned—the idea of taking the domain name of a website, which is the information before the first slash. Potentially, that could be quite intrusive and could reveal a whole lot of information. It is not as innocuous as just bbc.co.uk, which is the example that they gave. For instance, that domain name could be saveyourmarriagelikeme.net or domesticviolenceservices.com. Maybe one of the most interesting ones is crimestoppers-uk.org. This is where you can make anonymous tips to help to solve crimes. Of course, if you had the Internet connection record that said that someone had gone to crimestoppers-uk.org and you also knew the time when the tip had come in—if you were the police, for instance—you could very easily figure out who had put in that tip. That is a real problem, because if you are destroying that anonymity you can undermine the ability to solve crime.

Q131 Mr David Hanson: This is the central question many of us will have to wrestle with. Surely the police, the security services or whoever accesses that, under authority, with judicial review, is doing so only because there is some potential link to a potential investigation. The vast majority of people will never have that link checked or looked at. I am wrestling with that myself. I want to get your assessment of whether the proportionality is there. If we do not collect the information, none of those leads can be followed up.

Shami Chakrabarti: You are collecting huge amounts of sensitive information that is not currently collected and, therefore, you are creating the vulnerability I am so concerned about. I am not even talking at the moment about potential abuses by the authorities. I am talking about the vulnerability to hacking by other people that you create when you create a massive sensitive database and put the entire population's online life under surveillance in this way.

Renate Samson: My understanding is that this would help to support requests that are already made for communications data. At the end of November, IOCCO published as a starting point to a further publication a breakdown of 100,000 communications data requests by 29 police authorities, including the National Crime Agency; 46% of those requests related to burglary, robbery, theft and drug offences. If this is to support that, people may see it very much as an intrusion. On that sort of issue of crime, why do you need to know what website somebody has looked at with regard to burglary? We have to think about the intrusion into people's lives, based on us as digital citizens, before we start to discuss the retention and use of Internet connection records. Their retention is an issue I know you have looked at, but off the back of the TalkTalk hack, for example, we need a lot more clarity on how companies will be asked to store that data to ensure that they are safe.

Jim Killock: You also have to consider the wider effects on society. If I said to you, "When you go home, can you note when you got home and which newspaper you read, although do not worry which article it was? If you ring your family this evening, make a note of that and then tomorrow, hand it into the police", you would think that an excessive ask.

Shami Chakrabarti: And every hotelier, every restaurant owner, every pub, every cinema and every theatre that you enter will be required to keep a record of when and where you entered. That is the equivalent of what is being proposed.

Jim Killock: The question then is, is that a proportionate thing? What are we trying to solve? Is it quite as desperate a situation as is being claimed? As I said, these powers do not exist in other democratic countries. Russia has just been given a bit of a rap for similar sorts of activity. A number of European countries have rolled back on traditional data retention, never mind this kind of extension.

The Chairman: Lord Strasburger?

Lord Strasburger: My point has just been covered.

Q132 Stuart C McDonald: Are there other ways to go about IP resolution that are less troubling? The Home Office and law enforcement agencies will say that retention of these connection records is essential for that to be successful.

Jim Killock: One thing that you have to ask is whether the technology will out-evolve this. Will IPv6 catch up with some of the problems that it is currently seeing? You also have to ask how the Internet might work in the future and whether any of this will work. Some of the evidence that has been put about is quite interesting. People have said, "How do we know whether somebody has used Twitter or Facebook? We need to know in emergencies whether somebody has been accessing that website". Phones just do that now every couple of minutes. If they are constantly connecting to all these services, you will just have a huge glut of information that is not a fat lot of use to anybody.

Q133 Matt Warman: One of my frustrations with this conversation is that it is always said that the Government are being asked to hold this stuff. Actually, we are asking ISPs to hold it. That is a very important distinction that we need to continue to make. Law enforcement agencies tell us that they want access to the information and are happy for it to be held externally. You seem to be saying that you are not happy with that. I wonder what alternative you would propose.

Jim Killock: It may not be a government-held database, but it is a series of data centres that are all accessible by a single mechanism that can then be queried in parallel from an officer's desk.

Matt Warman: With appropriate oversight.

Jim Killock: There are some interesting things there. It seems that the way it will work is that you can get an officer to ask the computer whether it has any useful information in a case. It will tell you the things that it might have, and then you can go off and get some warrantry for it. It is almost saying, "We will go not on fishing expeditions, but if you did, here are the results you would get. Why don't you have a think about whether or not that is useful?".

Renate Samson: You say that there will be appropriate oversight. Currently the Bill will retain the process that we have now. From Big Brother Watch's point of view, that is not

appropriate oversight. We would like to see a further layer of independent judicial approval and authorisation of an internally signed-off warrant.

Matt Warman: The point I was making is that it is not a free bucket any policeman can look at.

Renate Samson: We also have to acknowledge the recent case with regard to Police Scotland and on which IOCCO reported, where warrants were being signed off and misused.

Matt Warman: Misused being the operative point.

Renate Samson: Yes.

Shami Chakrabarti: Sometimes that will happen. To go back to the real-world analogy, when I said that this is the online equivalent of requiring all those businesses—hoteliers, restaurants, cinemas and so on—to keep a detailed record that they do not currently keep of everybody's comings and goings, that does not mean that I am against ever putting a particular hotel, restaurant, gym or whatever under surveillance. I just think that you take a targeted approach. When you get suspicion that conspiracies are being conducted in a particular room above a particular pub, at that point you put that site under surveillance. Then you put the people who have been to that site under surveillance. That is the kind of approach we should continue with in our democracy, in the virtual world as well as the real one. If you have concerns about particular activity and sites, you can go to ISPs and CSPs and ask for the data they currently hold anyway. You can seize people's devices, because those people or organisations have now come under suspicion. You can target suspicion not just around individual people but around organisations and, indeed, websites.

Renate Samson: I want to clarify your point about misuse. IOCCO is very clear that judicial approval was not obtained to acquire the communications data. My point, and the point of Big Brother Watch, is that independent oversight and authorisation of an internally signed-off warrant for communications data would, I hope, potentially ensure that misuse did not occur. That is just for clarity.

Jim Killock: The important thing is why we have the idea that necessary and proportionate surveillance is essentially targeted, rather than blanket. Why do we have that rule? Why has that been pushed forward? It is easy to imagine that in the UK we will never have any problems with our democratic institutions, the police will never overstep the mark and we can solve all this through authorisation regimes. However, if you look over the sea in France, you have the potential of a Front National Government, with parallel powers. You have powers similar to these in China and Russia. Is it the role of the UK to say that blanket surveillance, easy profiling and access to everything that everyone does in their lives is the right international standard to set and is absolutely, 100%, guaranteed never to turn into a problem in this country, or should we restrain surveillance to somewhere we can trust, for ourselves, for other people and for the long term?

The Chairman: Can I move to Lord Butler?

Q134 Lord Butler of Brockwell: I want to ask you about equipment interference. You have made reference to that. As I understand it, you are not claiming that equipment interference in the past has been non-statutory. You are claiming that, although there are statutory powers, they are very general, they have been widely interpreted and the public have not been aware of what is going on. Do I have your argument right?

Shami Chakrabarti: You do have my argument right. I do not believe that equipment interference was necessarily in the mind of the legislators when the provisions that are now being relied on were passed. Those provisions were more about traditional breaking and entering, bugging and so on. I certainly do not think that the public understood in that way the activity that was being justified ex post facto. That creates a problem for Article 8 of the convention, which requires a certain level of public understanding for something to be law for the purposes of the ECHR. Those powers were there and they were used for more traditional interferences, but hacking is a very, very serious business. It is more than just surveillance, because you are potentially changing data and causing long-term damage to data security. I am not saying that it should never be allowed, because that would be like saying that you should never break and enter in order to find the hostage, the terrorists and so on; I just think that there should be much tighter safeguards for hacking in the Bill. Again, in principle, it should be a targeted approach, not a blanket one.

Jim Killock: It is worth remembering that the hacking power has already caused some very significant problems. You probably remember that Belgacom, the telecoms provider in Belgium, was hacked by GCHQ, allegedly. In the first month of the clean-up, that cost it around £15 million. A series of telecoms providers, including Deutsche Telekom, were also hacked by GCHQ. Those are law-abiding companies. They are not terrorists. They have information and are a conduit to further information, perhaps, but they are also people who can be compelled to co-operate with their own national authorities. However, GCHQ, under this warrantry and hacking regime, has instead taken the view that foreign, legitimate companies with international stature, within the bounds of Europe where we have common laws and systems, are a legitimate target for hacking, and that the clean-up operations are, frankly, not our concern.

Lord Butler of Brockwell: Could we stay within the UK for the moment?

Jim Killock: But this is a UK operation.

Lord Butler of Brockwell: I know that it is a UK operation. I am just talking about the targets at the moment. The point that you have made is about overseas targets. That is a separate consideration. Within the UK, you must agree that it is an advance that this proposed Bill gives specific authority for and introduces transparency into that power.

Shami Chakrabarti: I agree with that. I wou*l*d just like it to be more tightly regulated, given the consequences.

Lord Butler of Brockwell: Sure. You are not arguing, are you, that such a power, properly warranted—we have had discussions about what proper warranting is—may not be a legitimate weapon?

Shami Chakrabarti: In extremis. The intrusion is graver, because it is not just surveillance but actual damage—not least, potentially, damage to fair trials, if now every criminal defence lawyer can argue, "This isn't a genuine email. This isn't genuine data any more, because of hacking capacities". Given how serious the consequences of hacking are, the thresholds possibly need to be even higher than for other powers in the Bill.

The Chairman: I will now move to Lady Browning and Lord Henley. I am conscious that there is a vote in the Commons at 7 pm, but I would very much like the Commons members to be here for the questioning.

Q135 Baroness Browning: You have all expressed concern about Clause 189. I wonder whether you could share with us what you believe the effects will be on both service providers and customers. Ms Wilson Palow, your submission stated very clearly your concern about this.

Caroline Wilson Palow: It is a very broad power, to begin with. Essentially, it says that obligations can be placed on service providers to facilitate interception, hacking or any other power in the Bill, and they would need to take those steps ahead of time, before an authorisation or warrant was placed. Within that broad power, there are some examples of what might be done. A particular concern of ours is the removal of electronic protection. We interpret that as the potential to undermine encryption. Encryption is crucial to so much of what we do all the time, including all our financial transactions. It gives us the security to operate online. The removal of encryption has the potential to undermine all of that. We think that the balance there has not been struck appropriately.

Shami Chakrabarti: Taking my real-world analogy again, because of my poor understanding of these things, I do not think that it would be proportionate to give government the authority to demand that every locksmith in the country makes a spare key every time he is setting a lock for a home, a property or whatever. It is proportionate in certain circumstances, under warrantry, for the authorities—the police—to break into a targeted property because we believe that there are explosives, contraband or evidence there. To ban privacy, to ban private conversations and to require people who live on trust—companies that are all about creating a space of trust, so that we can have trust in our banking system et cetera—to leave those gaps in the nation's cybersecurity is quite problematic.

Renate Samson: It is the point that we were making earlier. The Bill is about protecting society. Encryption enables the protection of society. It enables people to use Crimestoppers. It enables whistleblowers to lay clear things that are going on that benefit society. It enables the vulnerable to communicate safely. Battered wives, for want of a worse expression, can ensure that they communicate as necessary. People on witness protection programmes can have an element of safety. It is much broader. It involves all of business. When all the communications in our home and everything else we have talked about on the Internet of things are connected online, we all want to know that our energy can be supplied safely. Encryption, as our submission to you explains, is not just a concern of privacy campaigners. It is a concern of Governments and business and one that will impact on us all, as all our lives are lived online.

The Chairman: Thank you very much. I move now to Lord Henley, on the Wilson doctrine and other matters.

Q136 Lord Henley: There is protection in the draft Bill for legally protected communications of journalists and journalists' sources, and there are protections for Members of Parliament of both Houses, enshrining the Wilson doctrine. Do you think that the Bill goes far enough?

Shami Chakrabarti: Not at all. There is room for some serious improvement. Let me be positive: there is room for real improvement. As far as I can tell, the Wilson doctrine has been completely reneged on. Recent statements by the Prime Minister suggest that, effectively, there is no Wilson doctrine in practice any more.

Lord Henley: What particular comments of the Prime Minister are you referring to?

Shami Chakrabarti: My understanding of recent statements from the Prime Minister is that there is now no absolute practice of not intercepting parliamentarians' communications. That was an absolute promise that came from Prime Minister Wilson and, indeed, was repeated by subsequent Prime Ministers.

Lord Butler of Brockwell: No. I am sorry, but you are wrong about that.

Shami Chakrabarti: I have read the Wilson statement. As regards what could be improved, I accept that there could be certain very rare circumstances where it would be justifiable, in a democracy, to interfere with even the communications of parliamentarians, lawyers and journalists, but we want something closer to the provisions that you currently have in place for production orders. You want something approaching reasonable grounds for believing that a very serious criminal offence is happening or has happened, and that there are no alternative ways of getting to the evidence; otherwise there are real dangers. Think of the political dangers. Perhaps it was just a rhetorical flourish, but we have had leaders of parties suggest that opposition parties are a threat to national security. I do not think that it is healthy for democracy for opposition political parties to believe that it is possible that they can be intercepted just on the say-so of a political opponent, even if that political opponent is the Prime Minister.

When it comes to legal professional privilege, we now know, because of the Belhaj case, that the security agencies were looking at legally privileged material that was relevant to a case being brought against them in relation to torture. There need to be much graver safeguards—we are back to judicial warrantry—and a very strong presumption against looking at parliamentarians' communications, legally privileged communications and journalists' sources.

The Chairman: Thank you very much. I will give you just one or two more minutes, because I want to wrap up with a couple of suggestions about how you can give us more evidence.

Jim Killock: I want to say something very specific about this. It is very hard to tell where the boundary between journalist and non-journalist lies. In this day and age, it is not somebody who is working on a paper; it could be somebody writing a blog and self-publishing. Many NGOs have a similar role to journalists in exposing, commenting and publishing. Particularly with communications data, where the system sometimes has to go to a magistrate or

whatever and sometimes has to be self-authorised within the police, it breaks down when you have this blurring, which is a very strong reason why all authorisation should be done by an independent authority. That, in particular, has been spelt out in the data retention judgment by the CJEU; when communications data are accessed—in that case, it was talking about retained data—there should be independent authorisation. This is one of the reasons why.

The Chairman: Thank you very much. It has been a fascinating session. It really has—very revealing. If in the evidence that you present to us you want to go into some of the detail of any amendments or drafting issues that you feel would improve the Bill, which you mentioned earlier, please feel free to do so and send those suggestions to us. Thank you very much for coming along today.

William E Binney, retired Technical Director of the United States National Security Agency (QQ 234-249)

Evidence heard in public Questions 234-249

Oral Evidence

Taken before the Joint Committee

on Wednesday 6 January 2016

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins, Suella Fernandes MP, David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Bishop of Chester, Lord Hart of Chilton, and Lord Strasburger.

Witness: **William E Binney**, retired Technical Director of the United States National Security Agency, gave evidence.

Q234 **The Chairman**: A warm welcome to you both. Welcome to the British Parliament. We are dealing with a very important piece of legislation that we have been asked to look at by the House of Lords and the House of Commons. We are very grateful to you both for travelling to give your views on some parts of this legislation, and I thank you both very much indeed for coming along. I shall start the question session with a very general question to you both. If you wish to make general points about the Bill it may be appropriate for you to do it at this point. Do you think that this Bill is necessary at all, and do the provisions of the Bill strike the right balance between privacy on the one hand and security on the other, which is the eternal question?

William E Binney: First, I thank the Committee for giving me the opportunity to come and give testimony. I hope I can help you with some of the issues you are discussing in this Committee. My big objection with how NSA, GCHQ and the law-enforcement agencies affiliated with them deal with data is fundamentally about the bulk acquisition of data of any type. When I became the technical director of the world analysis and reporting group at NSA, which had about 6,000 analysts and was responsible for reporting on every country in the world, I had to look at the major problems that they were facing and try to figure out ways of solving them. I took the position in 1997, when the big explosion of digital communications was occurring, so the biggest issue I had to face was that explosion and how our NSA analysts were dealing with it. This was also true at GCHQ. GCHQ and NSA basically do the same thing, so they co-operate very closely. If one has a problem, the other does, and they have the same problems. The issue was that our analysts, even back then in the 1990s, could not see how to resolve issues around the world because there was too much data for them even to look at. That was before we had the bulk acquisition of data we have today. Back then, we were collecting the smallest lines of communication. We could not deal with the fibre rates. We did not invent that. A little lab I had, the Signals Intelligence Automation Research Center, invented the ability to pull back together and recompile everything going at fibre rates in 1998. At that point, we deployed that, creating problems that were orders of magnitude greater for the same analysts because they were

still doing dictionary select routines that would look through data and pull out anything that matched the dictionary. That basically pulled in everything, dumping all that data on the analysts, so they could not see the forest for the trees.

That was the fundamental problem. The way I approached that was to ask what was the fundamental issue that would solve the problem. It boiled down to looking at the metadata that was used to transport the data around the networks, and there were only two networks to deal with. One was the public switch telephone network, using cell phones, landlines, satellite phones and so on, and the other was the internet. In the case of cell phones, they are run by the International Telecommunications Union and are organised into nine zones around the world. The internet is run by ICANN and IANA. IPv4 and IPv6 basically tell how data is routed across the network, where the terminals are and who they are. It is the same as a telephone number, except the internet is divided into five zones, not nine, and the numbering is blocked and allocated in sections of blocks. I have information on that that I would like to share with the Committee so that members can look at it at their leisure to help them understand the issues.

Using that data gave us the ability to build social networks for everybody and see how they relate in the world and to use that as an upfront filter to sort out the data as it is passing the point of collection or of access. Our process allowed us to see into the massive amount of data. Our initial objective was to run at the order of 10 terabytes a minute, which, to give a scale, is several Libraries of Congress every minute. We were going to scale up from that because that is the order of magnitude of what is going on in the world of communications today. From that, we built this entire targeted approach. It gave us the known targets which we centred on, and then we used the social networks, the defined zones of suspicion around them, to give us a very finite number of targets to look at and pull out data. We were getting ready to apply other rules, but did not do so at the time. For example, if you had a satellite phone that could be located in the mountains of Afghanistan or the jungles of Peru, you fell into the zone of suspicion, so you were pulled in as a part of that. All this was run by code, automatically. We had no people involved in this process. That was what the Signal Intelligence Automation Research Center was all about. This was all done for about $3.2 million. That was the entire cost of that operation. It showed that you had to get away from dumping bulk acquisition on your analysts because that makes them fail, and that is consistently what has happened.

That is what I objected to from the beginning of this process at NSA. That has made its analysts fail, and they have failed consistently since 9/11 and even before then. My thrust is against bulk acquisition of anything. Let us do collection, analysis and reporting smartly. Let us do it in a directed way. That will give privacy to everybody in the world because you do not take in their data. You can filter it upfront. You can even sessionise it and recognise it at the packet level. You do not have to do it at the full reconstructive session. That is my thrust. The Bill should really address bulk acquisition and terminating that. That is really what I think.

Q235 **The Chairman:** Thank you so much. Mr Lund, would you like to give your views?

Jesper Lund: Thank you, Lord Chairman. I am glad to be here and to give evidence before the Committee. I will focus on internet connection records in my opening statements because in this area I have serious concerns about privacy and efficiency. This is probably

an area where the Bill does not strike the right balance between the two. It is tempting to compare ICRs with phone bill or call detail records, as they were formally called. This was also done in Denmark when our ICR scheme was introduced about 10 years ago, but there are a number of differences. The internet is simply not as structured as the telephone system, where you have a line in use whenever two people are communicating with each other, so you have a caller and a call party and a duration of the call that can easily be registered, and is usually registered for billing. For the internet, it is not as straightforward to do something similar and it is certainly not something that exists today. So, if you force communications service providers to do this, internet connection records will have to be formally defined, equipment will have to be purchased, and the data that you are going to get will probably not be what you would expect from a law enforcement perspective if you think about two people communicating via Skype or Facebook because the internet is a stateless system. Every communication is broken into packages which are transmitted independently. In principle, you can retain some information about these packages that are transmitted across the internet but it is going to be a really large database and highly unstructured. There is going to be a needle in a haystack problem every time you use this data.

In terms of privacy, since so much goes on on the internet nowadays, you are essentially going to store everything about the activity of British citizens, at least to the extent of their activity on the internet. Even if only a small fraction of that data will ever be accessed, citizens will still have the impression that, when they do something on the internet, information is retained about it, which was not the case before, so there is a substantial proportionality issue here that I think should be addressed. In terms of necessity, internet connection records may not be as useful as you would think in the first place. I am sure we will come back to this on questioning, but the Danes' experience, which was based on the same objectives as this Bill, ended up with the conclusion that internet connection records were really not useful for law enforcement work. They were barely used and after seven years a similar system, which, I should point out, was perhaps less ambitious, was scrapped in Denmark. However, it was less ambitious because of cost, so doing something that could potentially be better would also be more costly.

Q236 **Suella Fernandes:** I want to look at the comparisons between the Danish experience and what is proposed in this Bill. Mr Lund mentioned cost. Would you agree that one of the big differences was that in Denmark the equipment cost of data retention was borne solely by the communications service providers, whereas there is a very different approach under what is proposed in this legislation?

Jesper Lund: Yes, I understand your question. It is true that certain compromises were made in Denmark because the cost of the equipment was borne by the communications service providers. The limitations that have been pointed out by the Ministry of Justice in its self-evaluation report affect only about half of the customers that the internet connection records are concerned with, so if there was a case for using this system it could certainly have been proved. As regards the other half of the customers, where problems turned up at a later stage because of some compromises that were made early on, some but not all the customers were affected, so if there was a case for using internet connection records I think they should have been able to prove it with the Danish system, even given the compromises that were made.

Suella Fernandes: Would you agree that cost was a key factor in the options used, whereas in the UK legislation that cost is not such an important factor?

Jesper Lund: Perhaps I should explain to the Committee what compromises were made. The main compromise in Denmark was that communications service providers were allowed to retain internet connection records at the boundary of their network, which is normally not a problem. It was not seen as a problem in 2005 because at that time the sharing of IP addresses was fairly limited. But since we have had more devices using the internet, especially smart phones and tablets which need lots of IP addresses, we have sharing of IP addresses and when the connection is done at the boundary of the network it is sometimes impossible to distinguish between different customers. That was certainly a limitation and was a factor in the limited effect of the Danish system. I should also point out that it affects only roughly half of the customers who were subject to internet connection record retention. I say again that if there was an operational case for using internet connection records in police work, the Danish law enforcement authorities should have been able to prove it for the other half of the customers where these limitations should not really be a problem.

Suella Fernandes: Just lastly, on a point of comparing capabilities, would you agree that the UK has extensive experience of delivering central systems and in training law enforcement and technical capability, whereas the evidence has been that it has been more limited in Denmark?

Jesper Lund: I certainly agree about that. It is true that the evidence for using internet connection records in Denmark is not so good. However, there is other evidence on the use of other types of data retention by the Danish police which shows that it is highly professional and done quite well, especially call detail records and locating information from mobile phones, so I would not say that the Danish police lack technical skill in using data retention for their work. My interpretation would be more inclined towards saying that internet connection records are simply not as useful as was thought initially.

Suella Fernandes: Mr Binney, how would you compare the capabilities between what is proposed in this Bill and US powers?

William E Binney: Well, the US has an awful lot of resources around the world. I mean it has implants on switches and servers around the world; the latest publications stand at over 50,000. I believe that with the latest collection of SIM cards that GCHQ did, plus some other stuff that NSA does, they probably have millions of other access points. That is really intruding into the system in an active way on a massive scale. But again, the end result is so much bulk data that analysts cannot figure out what they have. That is the real problem. The problem of doing intentions and capabilities predictions—that is, the threats from attacks and so on—is an analytical problem, not a data problem. It takes data to figure things out but you have to be selective in it because the selective targeted way gives you a rich environment of information to figure out what attacks are going to happen. If you put all that bulk data in, it covers it up and people cannot see it. That is the problem they are having today; that is the problem they have always had. That is why we did the programme to try to solve that back in the 1990s, and that is when we did solve it.

Q237 **Victoria Atkins:** May I just clarify Mr Lund's evidence? You have told the Committee that certain compromises, to use your word, were made. Am I right in understanding your evidence that those compromises meant that 50% of customers were essentially in the dark—they were black—to the security services through the collection of the ICRs you have described?

Jesper Lund: Yes, I am not sure that it was precisely 50%, but in all cases IP addresses were shared, so it was basically everyone who accessed the internet from a mobile device.

Victoria Atkins: You used the word "compromise"; another way of putting it is that the system employed by Denmark, with the costs borne by CSPs, is in fact half as effective as the system proposed in this Bill. Would that be a fair way of putting it?

Q238 **Victoria Atkins:** You used the word compromise; another way of putting it

Jesper Lund: That is one way of putting it, but it is still the case that for the other half of the customers, these limitations and compromises should not really affect the potential for using internet connection records for investigative work, even in those cases where the police are unable to come up with realistic cases of the use of such connection records.

Victoria Atkins: But if the system is so flawed in the first place that they cannot locate 50% of their market, it is not very surprising that they rather lose faith in the system, is it?

Jesper Lund: Maybe not, but I would still say that for what we call fixed lines for internet access in private homes, these problems, because of collection at the boundary of the network, should not really affect the potential usefulness of internet connection records. Still, neither the police nor the Danish security and intelligence service, which is our version of MI5, have been able to come up with concrete cases of using internet connection records to determine what communication services people have accessed, for instance, which was a deliberate goal. The Danish police have stated in evidence given to the Danish Parliament that what they usually do instead is seize the laptop or smartphone of the suspect and investigate that device, instead of getting access to internet connection records. They did not give their reasons for doing that but presumably it is because of the extremely large data set that they would get if they retrieved internet connection records from communication service providers and they would be searching for a needle in a haystack, whereas presumably the information that can be obtained by seizing the suspect's laptop or smart phone and searching that is of much better quality for the police investigation.

Victoria Atkins: That is two issues, if I may say so, and indeed law enforcement in this country seizes devices where it is able to. However, the devices are not always available, and we have heard from other witnesses about that. I just want to pin you down on the point about the differences between the Danish and British systems. If a terrorist or a paedophile happens to be in the dark 50%—in other words, the 50% that is not available to Danish law enforcement—then they are not going to be detected under the system as deployed under the Danish method. Is that right?

Jesper Lund: That is true for the system of collecting internet connection records that is no longer in place.

Victoria Atkins: If I understand your evidence correctly, the reason why these compromises happened in the Danish system was that the commercial service providers were bearing the costs, and they wanted to get away with paying as little as they could. Would that be a fair analysis?

Jesper Lund: I would say yes, but in the end the Danish communication providers are of course going to do what they are ordered to by law, so if Danish politicians had really wanted a more extensive system they could have obtained that. The cost of the Danish system, if you take the cost of the system that is no longer in place and scale it up to the UK, is something between £15 million and £20 million per year. Multiply that by 10 and you have something like what is budgeted for the British system under the Bill, with the compromises that in the end will no doubt have some negative effects.

Victoria Atkins: So that I am not asking you questions that do not fall within your expertise, do you have any knowledge of the business relationship between commercial providers in the UK and law enforcement? Are you aware of how well they work together?

Jesper Lund: No, I am not.

Victoria Atkins: No. Looking again at the Danish situation, then, is it fair to say that the relationship between the commercial providers and law enforcement is not as strong as has been indicated in the course of these evidence sessions? We have heard from Vodafone and others about the interactions that they have with commercial providers here in the UK.

Jesper Lund: Danish communications providers follow the law, of course. They also work together with the Government on setting up systems that are manageable. So the history of the Danish system for the collection of internet connection records was not just a matter of cost; it was initially a matter of the Minister of Justice wanting something that was technically unfeasible. I see signs of the same thing in this Bill. For instance, it is mentioned that an internet connection record could be the destination IP address or the server name. It is certainly possible to define internet connection records in terms of both IP addresses and server names but, in terms of complexity, and hence of the cost of running these systems, there is an order of magnitude in the difference between requiring communications service providers to retain the internet protocol address and doing the same for the server name. The first is pretty simple, but asking them to retain the server name is asking them to do deep packet inspection because the server name is not really available to them. What they get is a packet and an IP address, and then they transmit that packet to the IP address. To get the server name they will need to do some form of deep packet inspection, which is a lot more costly than simply retaining the server name. There was collaboration between the Danish telecommunication industry and the Ministry of Justice, to the benefit of both parties.

Q239 **Lord Strasburger:** Good afternoon, gentlemen, and thank you for travelling as far as you have. I think I have a pretty good idea how you are going to answer this question, Mr Binney, but I will ask it anyway. Is there a good operational case for the provisions in the draft Bill on bulk interception, bulk acquisition of the collection of communications data and equipment interference?

William E Binney: My short answer to that is no. The reason for that, again, is that in each of those cases, no matter what you do, you are capturing so much data. For example, GCHQ alone wants to collect between 50 billion and 100 billion records per day on certain aspects of communication. That dumps 50 billion to 100 billion events or activities on all their analysts, but they may produce 1,000 or 2,000 analyses at most. If they use the standard approach of doing a word search, which is what the NSA does but is the wrong approach, what happens is that when they look at content from the internet, from transcribed phone calls or indeed from anything by either machines or people, they get so many matches it is like getting a Google return—every time you submit a Google query you could get 100,000, 1 million or more returns—and that is just from the input for that day, and every day is the same. That means that the analysts cannot get through the material, which means that they fail to see the threats. The end result is dysfunctionality among the analysts and no prediction of intention or capabilities, no stopping of attacks, and people die. Then when they die, you find out who did it, and then you focus on those people. That is when you do the targeted approach, like the French are doing now—they are going after people and raiding them because they went after the people who had done the attack and looked at who they had relationships with from the bulk acquisitions that they had. They could have gotten all that data upfront through a targeted approach, and could have had the opportunity to stop the perpetrators before the attack. That has been true in all these cases. We have even proved that it was true with regard to 9/11. The NSA could have done that too.

Lord Strasburger: The Home Office argues that it is essential in the modern world to give the agency every means available to find needles in haystacks, in order to keep us safe. Is that correct?

William E Binney: My response to that would be that it is not helpful to make the haystack orders of magnitude bigger, because it creates orders of magnitude of difficulty in finding the needle. That is really the issue. Using a targeted approach would give you the needles, and anything closely associated with them, right from the start. That is a rich environment to do an analysis on, and it would help the analysts to succeed in predicting intentions and capabilities.

Lord Strasburger: Would any alternative approaches to these bulk powers be more proportionate and effective?

William E Binney: Yes. It is called the targeted collection approach, using the ability to look into the data that we currently have with devices such as Narus and Verint and various other commercial devices, and then giving it sets of targets to look at as well as defining zones of suspicion around it. That would manage all the data input and selection or collection out of the data flow. It means that you get that smart, rich environment for analysts to look at and analyse, and it costs a minuscule amount—probably one-hundredth of what they are spending now.

Lord Strasburger: Does the presentation that you have given us refer to what you call targeted collections?

William E Binney: Yes, and it shows how to do them.

Q240 **Bishop of Chester:** I find the evidence this afternoon fascinating, because in a sense you are attacking the engine room of the Bill. It is like an Exocet targeted on it.

William E Binney: I always do things in a targeted way.

Bishop of Chester: I imagine this as an aircraft carrier. It will be a very big one when all the data comes in, and it is vulnerable. Let us assume that I am convinced you are right—I am certainly very interested in what you are saying. Why do you think that the British Government, with all their GCHQ experience, their relationship with the NSA et cetera, have taken this approach, which is so diametrically opposed to what you advocate?

William E Binney: I think I know exactly why. They took it because the NSA did. The NSA did it because of contractors and the interests of contractors in getting money and feed-in. There was an awful lot of money upfront, like $3.8 billion, to start the Trailblazer programme, for example. If you want to look that up on the web, it was the one where they started to do capture of data on the internet alone. There were other multi-billion dollar programmes that followed it and were associated with it. So there is an awful lot of money behind the scenes that the contractors wanted to feed on. They all lobbied for this approach because it took so much more money to do. That gave them the opportunity to get more contracts and feed-in. I called that relationship between NSA and the contractors an incestuous relationship because people would retire from NSA and go work for the contractors and use their influence to get contracts and things like that. That was the way NSA took it. I publicly accused it of this, of trading the security of the people of the United States and the free world for money. This is why it did that.

Q241 **Mr David Hanson:** I am interested from both of you what the balance is. You indicated that bulk collection and its analysis has some potential value but it is needle-in-haystack value. On the same side, we have the targeted approach, which would follow through particular leads. Currently, what is the balance in terms of government activity on that?

William E Binney: Currently, there is not too much of a balance unless there is an attack, for example the recent attacks in Paris. Take those two attacks as the case in point. After the first attack, they went to bulk acquisition. How much good did that do them in helping to prevent the second attack? It did not help, but they started getting and finding people once they found out who did the attack and focusing in on the data they already had accumulated on those people, which they could have got originally from a targeted approach upfront instead of waiting. By doing that, now they find other people and are potentially stopping future attacks.

Mr David Hanson: We have had evidence from police and other agencies saying that the targeted approach cannot work now because, effectively, a range of material is in Facebook, Twitter, the dark net and other forms of media. The purpose of bulk collection is that we do not know who is involved in that until there is a lead. The lead follows through to accessing bulk collection material. Is that valid?

William E Binney: I understand that, but with the dark web, when you put a tap on the fibre line, you get the entire fibre line—whether it is the dark web or not. If it comes across the fibre, you get that data.

Mr David Hanson: But the justification that we are getting is that to have an effective targeted approach to people involved in or accessing terrorist, criminal or paedophile activity, or whatever it might be, the agencies need to have access to any record. Any record means anybody in this room's record, but actually it would ultimately only focus down to the record of one person in this room because they were the person we were interested in.

William E Binney: I understand that that is the objective of intelligence, too, to be able to do that. Again, the issue is doing automated approaches for analysis of the data upfront. That really gives you the ability to sort that thing out. For example, if you want to look at terrorism, you want to look to networks that use the internet or phone to communicate. You look for zones that connect certain parts of the world, such as certain countries. You can automatically do that with software, which is what we were doing, but they did not particularly opt for. That was their option and they picked it because of the money involved. You can automatically do that with software but when you reject the smart approach to targeted analysis, processing of data and analytic processing, you reject the opportunity to solve those problems upfront. Then you end up getting only bulk data because it is, "I know nothing so give me everything". That is what you are saying when you do bulk collection: "Give me everything so that I have the opportunity to find out".

Mr David Hanson: I think that we had it put to us that it is, "I do not know everything but I need to access something which I cannot currently access".

William E Binney: I would say that that is false. They can currently access anything they want. When you tap a fibre, you have access to everything. When you go to an ISP or the telephone company, they have access to the entire network. You can tell them to give you any number or any switch they have got, or they can use the implants they already have in place to do that. That is not an issue.

Q242 **Victoria Atkins:** Just to be clear, Mr Binney, it is 15 years since you worked for the NSA, and your security clearance was removed before you resigned in 2001.

William E Binney: I did not resign; I retired.

Victoria Atkins: On leaving the NSA, you co-ran a consulting company providing intelligent security computer analytics. Is that correct?

William E Binney: It was called Entity Mapping, LLC, yes.

Victoria Atkins: I do not have any view on this, but when you describe an "incestuous relationship" between NSA and contractors because employees from the NSA go to contractors, it could be said that you profited from your role at the NSA after you retired.

William E Binney: We never attempted to get into contract with the NSA. We only did it with NRO, CIA and Customs and Border Protection.

Victoria Atkins: What is this document?

William E Binney: It is the way to do targeted analysis and reporting, and gain a rich environment for an analysist to get data off the network.

Victoria Atkins: Is it a computer program?

William E Binney: It is in the form of a computer program, yes.

Victoria Atkins: And who owns it?

William E Binney: The company name is TDC, the Technology Development Corporation, which has the set of software to do the sessionising of the data. We had at one point the software to do the analysis of it but we left that with the Government.

Victoria Atkins: Just so we are clear, do you have any commercial interests still in this area?

William E Binney: No, I am not in business now at all.

Victoria Atkins: Okay, thank you. Following on from David Hanson's questioning, we heard from a number of law enforcement officers and security services witnesses who are at the rock face now, not 15 years ago. Their evidence has been that they need these powers. Are you telling this Committee that each and every one of those witnesses is wrong, and indeed possibly misleading the Committee?

William E Binney: I guess I am.

Q243 **Shabana Mahmood:** I want to come back to internet connection records and you, Mr Lund. Obviously, we have had quite a long discussion already about the Danish experience, its usefulness and your opinion of that. First, I want to touch back on this point about the 50% data that were not available in the Danish system, which I think you defined as everybody who accessed the internet on a smartphone.

Jesper Lund: Yes

Shabana Mahmood: So the argument is that the Danish example is not helpful because there was this whole bunch of data that could not be accessed and therefore it does not tell us anything about what we are trying to do with internet connection records in this country. But is it not the case that even if in the Danish experience they had been able to get that 50% of smartphone data and had complete coverage, as our system attempts to do, that data would have been potentially mostly useless because of the problem of constant connection and the fact that on smartphones the apps that police and other people would be most interested in are on a background app refresh and therefore constantly connected to the internet, which tells you nothing about when it has been activated? Would you agree with that?

Jesper Lund: Yes, you would be able to see that a person, for instance, uses Facebook or Facebook Messenger, but you would probably not be able to see when that person is communicating with Facebook Messenger because there is constant communication in the background between your smartphone and the servers at Facebook.

Shabana Mahmood: So that additional 50% that could have been collected but was not is probably not very useful anyway.

Jesper Lund: It is always hard to make statements about hypothetical situations, but I would still say that if there was a rational case for using internet connection records, Danish law

enforcement should have been able to prove that using the other half of the customers, where these limitations were not a problem.

Shabana Mahmood: Was there anything positive about the Danish experience? We have heard a lot about its problems. Did anything come out of that experience that you or other people in Demark have found useful?

Jesper Lund: No. Lots of data were retained for seven years, and Parliament was told several times that they were extremely useful for the police, but in the end, a self-evaluation report by the Ministry of Justice—not by some critical NGO that makes up a story about this—was not able to come up with a single operational case where internet connection records were used in investigating criminal activity. Even the Danish security and intelligence service, which was asked only about the quality of evidence, not about operational cases in an anonymised form, said they were of limited use to it. Initially, the Danish security and intelligence service, the Danish equivalent of MI5, was the mastermind behind our internet connection records system.

Shabana Mahmood: Thank you, that is helpful. From your submission, there is a suggestion that there are discussions about future proposals, possibly concerning internet connection records, in Denmark mark 2. What is happening with those discussions and what might a mark 2 scenario look like?

Jesper Lund: The Danish police and the Ministry of Justice want to get away from the simplified version of doing collection at the boundary of the network. They want to do it closer to the customer so that the information can always be associated with a specific customer, even when you have sharing of public IP addresses. The Danish telecommunications industry is highly critical of this because it will increase the cost substantially. I do not know precisely by how much, but it is by so much that the industry is opposed to it. If you translate that to the British scale, that would be greater than the budget that has been set aside for your internet connection records, the £170 million over 10 years. If they do that, it will be equally effective for fixed lines, where you do not have sharing of public IP addresses, and for mobile phones where you do. My suspicion is still that it will not be useful at all in the end, and that they will just have spent more money on the system. That is based on what I said earlier. If there was an operational case, Danish law enforcement should have been able to prove it for the customers that were not affected by the suspicions.

Shabana Mahmood: How would you say this potential second version in Denmark compares to the proposal in our draft Bill? Is it a similar range of powers this time and similar coverage? Will it be less or more, do you think?

Jesper Lund: It will probably bring it closer to what is proposed in this Bill. I have been in contact with the Danish telecommunications industry and it has had fairly limited discussions with the Danish Ministry of Justice about this. There has been a single meeting in 2015. I do not know whether the Ministry of Justice is going to propose this to Parliament. It could happen this year or next year. The Ministry usually consults the telecommunications industry to a greater extent before it does something like this.

Q244 Matt Warman: Mr Binney, we have heard repeatedly from various different agencies that they would always rather be targeted and spend the resources that you have described, which are much smaller, doing one very targeted thing, but that they want to have the option of having the haystack, as you put it, because that is the only way they can get to the people they need to get to in order to keep us safe. Your argument seems to be that they should be targeted, which they agree with you on, but that they should not have the option of the haystack. Can you explain how that would help?

William E Binney: The point is that they are interested in doing what they call target development, which is finding new people who are involved in that activity, whatever it is, whether it is dope or any other criminal activity – terrorism or so on. The point of doing the social networking reconstruction is that you can see those who are associated but not yet known. You can use other rules and smart things to do with software to look at the data to make assessments, such as the geolocation of positions and different things as they are passing by, and make a decision at that point about whether you want it. You can also put in other things. For example, you could classify as a target set all the known sites advocating jihad or any other kind of site you want, and look at who visits that site and how frequently they visit. That could put them in the zone of suspicion. That is how you do target development. That is really what they are after. You can do that in a targeted way with those kinds of rules added to it.

Matt Warman: That seems to be precisely what has been described to us. The ambition is not to have an infinite army of analysts but to have access to the pipe in order to target more effectively.

William E Binney: That is exactly what I am advocating, but you can do that upfront. You can make those decisions upfront, filter out all the other material, let it pass by and not even take it in. That gives privacy to everybody in the world and gets you the target set you want.

Matt Warman: Are you familiar with the request filter, as described in the Bill?

William E Binney: Yes, I think I am, but it is not the total Bill. You are still advocating bulk acquisition, and I am advocating stopping bulk acquisition.

Matt Warman: But, very briefly, it seems to me that the request filter filters out the bulk data. It does exactly what you are asking it to do. Are you saying that you do not understand that that is what the request filter does, or that you are not familiar with the details of how the request filter will work?

William E Binney: What I am getting at is that the bulk data is still stored and accessible.

Matt Warman: But not to the Government, thanks to the request filter.

William E Binney: You mean at the ISPs? The Committee needs to understand that there are many different things going on here that add to this bulk acquisition. It is not just the ISPs. If you look at some of the material that was exposed by Snowden, it shows clearly an upstream programme—the PRISM programme—looking at the ISPs contributing data upon request using a filter. The upstream programme captures everything directly off the fibres

as it passes by. That is the bulk data acquisition that is available to GCHQ through NSA and all the other resources that contribute to that.

Matt Warman: But that is not what is in this Bill and not what we are talking about today. PRISM is fundamentally different. This is not a Bill that proposes PRISM.

William E Binney: No, but PRISM is an analogy to filtering because it filters too.

Q245 Lord Strasburger: The common factor between just about every successful terrorist attack in Europe over the past 10 or 15 years has been that one or more of the perpetrators was known in advance. Are you saying that attacks such as 9/11 and 7/7 could have been stopped if the agencies had used smart collection instead of grabbing absolutely every bit of data that went by?

William E Binney: Yes. In fact, in the case of 9/11, Tom Drake, who took over the efforts that I started with Ed Loomis to do a targeted approach, took the program and ran it against the entire NSA database in February 2002, very shortly after the attack, with the knowledge that we had prior to 9/11 incorporated in it. That program pulled out all the data that was in the database that NSA did not know it had on the terrorists prior to 9/11, so it gave them all the alerts, all the phone calls to the Yemen facility, all the phone calls back to Hamburg and to Afghanistan, even all the internal relationships, and showed all the data about who was involved in the attack prior to the attack. That would have alerted them. The difference was that we were putting in automated algorithms so that when they hit something of interest and we knew it was of interest, the program automatically executed. There were no people involved in that decision. So the program would alert everybody electronically and pass reports to everybody who needed to know once something was detected. It was done in an automated software way. We did not have the impediment of having people look into databases to find what was important in the data and so on. That would have at least alerted people and given them the opportunity to stop 9/11. The same is true with all the other attacks because all these people were known and in knowledge bases already. If the agencies had done a targeted approach from the beginning and kept the data finite, their analysts could have found the threats. That is my point.

Q246 Stuart C McDonald: Turning again to internet connection records, we have heard Mr Lund's views about their practical utility. Mr Binney, if this Bill is passed, can you see internet connection records being of practical use to law enforcement and to security and intelligence services?

William E Binney: Not in the bulk collection way, no, because again you have the same problem: if you take in hundreds of millions of records, you have to have people looking through hundreds of millions of records to find what is important. That is why the White House issued the Big Data Initiative in early 2012, soliciting corporations to come up with algorithms that would find information in big data that was important to look at. They issued that initiative because they have this problem, too.

Stuart C McDonald: I can see that from a security intelligence point of view, but I turn to a law enforcement point of view. One example that law enforcement gives us is missing persons. They say that because telephone records are pretty hopeless, they would love to have access to a missing person's internet connection records to see whom they have been

communicating with. There are cases where they could have tracked a missing person more quickly if they had had the ability to do that. Do you recognise that as something that could be helpful?

William E Binney: Yes, and they can do that in a warranted, targeted approach. ISPs keep data for a short period of time afterwards, so it is still available.

Stuart C McDonald: What sorts of periods of time are we talking about?

William E Binney: I think that for most of them the figure with regard to their records is up to six months.

Stuart C McDonald: But do they do that? Is it a matter of practice?

William E Binney: Yes. On the web there is a list of companies' policies showing which ones keep data and for how long.

Stuart C McDonald: But at the end of the day you are accepting that there would be some practical utility in requiring the retention of records for six months.

William E Binney: Going after it in a targeted way, yes.

Stuart C McDonald: What do you mean by a targeted way, then?

William E Binney: Because you have at least the device that the person was using to connect with the internet, along with their phones and cell phones, so you have that data. You can use that data to go after them and data that was related to them.

Stuart C McDonald: Sure, but you would have to have retained en masse, because obviously you never know who is going to go missing, and then you have to go back.

William E Binney: The telephone companies keep that data for a period of time also, so you have that from them. You also have it from the ISPs for a period of time.

Stuart C McDonald: Okay. To both of you: what about the privacy implications of keeping internet connection records in the way proposed by the Bill?

William E Binney: To me, right upfront it destroys privacy. To return to the bulk issue, taking so much of it in destroys your capacity and makes your analysts dysfunctional. It makes your law enforcement people dysfunctional, too. They cannot find the data that is important.

Jesper Lund: In terms of privacy, you would basically be storing the entire internet activity of every British citizen, which is really intrusive. In the specific case of finding a missing person, what would be most effective would be if their mobile phone was still active; then the mobile telephone company can triangulate that phone using its mobile phone towers. If the phone is no longer active, presumably that is where a case could possibly be made for accessing internet connection records. However, those records may show you internet communications but they are not able to distinguish between active communications and

the background communications that would happen on a smartphone at any time, even if it was left alone in a different part of the country.

The Chairman: I remind the Committee that just before 4 pm I will have to call the Committee to order because of the vote in the Commons.

Q247 **Mr David Hanson:** Imagine for a moment that your objections are not listened to and there is a scheme in place under the Bill that operates as the Bill currently proposes. The Bill says that £247 million is available over a 10-year period for the running costs of the Bill. In your professional judgments, is that a feasible resource to meet the costs of the Bill as proposed?

Jesper Lund: If you want an ambitious system for collecting internet connection records, it will be more expensive than the Danish system. Extrapolating from the cost of the Danish system, taking into account the difference between the size of the UK and Denmark, the limited version that we implemented in Denmark would take up what is set aside for internet connection records, so I think it would be more expensive than £247 million.

William E Binney: I think that that might be a good estimate for the retention and storage of data. I am not sure that it would cover the cost of processing, interrogation and development of software to do all this and of managing the data once you have it, having analysts look at it, whether you need more analysts and so on. There are a whole set of costs that go with data acquisition.

Mr David Hanson: The costs are detailed in the Bill, but essentially the Government have currently allocated around £180 million for the costs of establishing the collection of bulk data. Is that reasonable for 70 million people over 10 years?

William E Binney: From my perspective, that should be reasonable.

Q248 **Mr David Hanson:** One final question. We have talked a lot about privacy. TripAdvisor, Facebook, Twitter, Hotels.com, Tesco, the Co-op and Spotify probably know as much about me as the Government do. Is that a problem, or is it just the Government you have a problem with?

William E Binney: I would say that all those companies cannot come and arrest you, charge you with crimes or retroactively do research on you. For example, if you take a position that the Government are not in favour of, you can become a target, as numbers of people have.

Mr David Hanson: I suppose my question is: is the bulk collection of data by all those private sector companies more or less objectionable than the bulk collection of data by the Government to stop terrorism, paedophilia, criminal activity, drug abuse and all the other activities? That is a conjectural point.

Jesper Lund: I understand the question. It is also one that has occurred to me several times in Denmark. The important difference is that you give consent to those companies to collect your data. You choose whether to use Facebook and you can refrain from using it if you do not have faith in its data collection practices. You cannot get out of internet collection records. They show your internet activity and they are going to be retained, whether you

want that or not. As I understand the British system, not all communication service providers will sign up to this, but you will never know whether the information is retained—

Mr David Hanson: I suppose that that also presumes that I am bothered about that. If I am not committing a crime, am I bothered about the fact that they could access it if I did? I just pose that as a question.

Jesper Lund: Sure, but my take on this is that privacy is a fundamental right that applies to the individual citizen, just like freedom of expression. Whether or not you want to use that right is your choice, but the mandatory collection of something like internet connection records infringes your right to privacy.

Q249 **Dr Andrew Murrison:** It has been said that the UK intrudes upon the privacy of its citizens in a way that practically no other western state does. I am concerned that the UK should be an outlier, if that is true. Clearly the point of safety is being with the pack; indeed, in a legal sense it is probably important that it is. What is your assessment of where this Bill would place us in terms of countries with which we can reasonably be compared in terms of the acquisition of data and the surveillance and control of that acquisition by the state? Sorry, that is a very broad and overarching question, and this is a very complicated Bill and there are parts of it that will apply to a greater or lesser extent in other countries. As a broad-brush approach, though, where do you think it would place us?

William E Binney: I think it would place you equally with the US, because this is exactly what the US does. It does it under Executive Order 12333, which has no oversight whatsoever in the US.

Dr Andrew Murrison: No oversight at all?

William E Binney: None at all, by courts, Congress or anyone. It is all done by presidential order. The Fairview programme is the primary programme for the collection of data against US citizens, and it has 100 tap points right across the US, distributed with the population. It is distributed in that way because it gives them the ability to capture all that data about US citizens. That is a violation of our constitutional rights and we have been trying to challenge it in court. They have been fighting like blazes to keep this out of the courts because they know that what they are doing is unconstitutional.

Dr Andrew Murrison: Presumably, that is a work in progress.

Jesper Lund: It is always hard to do these comparisons, even within Europe because sometimes the European Union has similar laws. My understanding is that the UK is at the forefront of data collection about its citizens in Europe. France is also stepping up the surveillance of its citizens but is taking different routes in certain areas—for instance, by forcing communication service providers to do some form of metadata analysis of the communications that are going through their systems, not just the retention of those communications. You see different approaches in Europe but my short answer would be that the UK is at the forefront of data collection.

Dr Andrew Murrison: In terms of intrusiveness?

Jesper Lund: In terms of intrusive data collection, yes.

Dr Andrew Murrison: And what about oversight?

Jesper Lund: It is probably even more difficult to do cross-country comparisons of oversight. If I compare the UK and Denmark, I would say that you have more oversight in the UK but also more data collection.

The Chairman: It has been a fascinating session for all of us. Thank you both so much for coming along and answering a diverse range of questions, and a double thanks for travelling from abroad.

Lord Blunkett (QQ 94-100)

Evidence heard in public Questions 94-100

Oral Evidence

Taken before the Joint Committee

on Monday 7 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Bishop of Chester, Lord Henley, Lord Strasburger.

Witness: **Lord Blunkett**, gave evidence.

Q94 The Chairman: We give a warm welcome to our colleagues, Lord Blunkett and Mr Paterson. First, we apologise to you. It is largely the fault of the House of Commons; it decided to have a vote and that put the whole business on by about 15 minutes. We are extremely grateful to you both for coming along to talk to us about this very important Bill. Because of your experience in government, both of you know a great deal about the issues involved, so we are very grateful indeed. I will take advantage of my position as Chairman by asking the first question, which is for Lord Blunkett and for Mr Paterson. It is a very simple one. Is this Bill necessary, in your view?

Lord Blunkett: I cannot promise to be anything like as riveting as the last session, Chairman. Could I declare a non-pecuniary interest? I have an interest in a company that is involved in verification and authentication in the payments business, so I have a bit of knowledge—not as much as your previous contributors, obviously—about what will drive companies out of Britain.

Yes, the Bill is necessary. It required updating, for the reasons that I spelt out in my written and oral evidence to the ISC, and if people have insomnia they are very welcome to read it. I will not repeat all that, except to say that we have moved from an analogue to a digital age. For some time, we have needed to update the former telecommunications procedures and safeguards for the age we are in at the moment. My precept has always been that we use the same principles. When I hear people suggest that somehow there is an issue with holding telecommunications data long enough to be able to access it when necessary, or that it is the same as the content, I wonder whether they would have used the same arguments if we were discussing this 20 years ago, in the telecommunications age that existed then.

The Chairman: Thank you very much. Mr Paterson, is it necessary, in your view?

Mr Owen Paterson: Chairman, thank you very much for inviting me to your Committee. Yes, I think that broadly it is, to bring the powers that our agencies have up to technological speed with our opponents. Having worked in Northern Ireland, as you did, I have no doubt

of the real dangers posed to our citizens on a daily basis. It is only right that we give the incredibly brave people who work in our security agencies every necessary tool in order to beat them. I totally agree with Lord Blunkett. The original principles should always prevail in how we oversee and manage this intrusion.

Q95 The Chairman: Before I move on to colleagues so that they can ask about interception and authorisation, which both of you are very knowledgeable about, I have one more question. A lot of the Bill covers bulk interception, bulk acquisition of collection of communications data and bulk equipment interference. Do you think that an operational case has been made for that?

Lord Blunkett: The term "bulk"—people talk about metadata—provides a fog around the issue. Surely the fundamental issue is that what is taking place requires monitoring. If monitoring involves collection of data, where should those data be held? Six years ago, the Government backed off the idea that there should be any attempt to hold centrally, so we are asking the private sector to co-operate. We are doing so in a way that allows the agencies to be able to do the job. We need to demystify this, if I may say so, because the term "bulk" worries people. The fundamental issue, which was touched on in your previous session, is what in a practical sense can be undertaken, and what meaningful information can be gleaned from it for acceptable purposes. If we drill down to that, we start to demystify it and can then challenge the agencies as to whether what they are doing is relevant to the objective that we have laid out for them.

Mr Owen Paterson: I broadly agree. Once the principle of interference and capture of private data is accepted, I am not worried whether it is a small amount of data or whether it is a bulk amount of data—which, as Lord Blunkett said, has become a bit of a shibboleth. The principle must be that this data are managed in a responsible manner. In my experience, our services have been punctilious in the manner they respect the constraints and the protocols put on them.

Lord Strasburger: On the subject of bulk, is it not true to say that the concern is not necessarily about the quantity but about whose data are being captured? There is a difference between surveillance or interception of the data of suspected criminals or terrorists and surveillance or interception of those of the rest of us. It is targeted against untargeted, rather than bulk against small.

Lord Blunkett: We have always collected them. They have been collected, have they not? They have been held. The records have been there, under the old telecommunications system. They were not accessible in the same fashion as they are now, at the speed they are accessible. Collation is possible, with new technology addressing new technology, but the process was the same, was it not? The data was held.

Lord Strasburger: It was not quite the same. In the case of telephone data, the data was held by the telephone companies for their own billing purposes. In the case of Internet connection records, we are asking the ISPs to create the data, which do not currently exist.

Lord Blunkett: We need, perhaps, to ask the ISPs, as you are presumably doing, what they do with the data, because the idea that they hold them now only for billing purposes is mythical. The amount of data that is used by ISPs for all sorts of purposes—people seem

willing to provide and to collaborate with that—is enormous. Just ask how much a Sky box provides, if we consider what is done with it afterwards.

Mr Owen Paterson: We are broadly in agreement again. Huge amounts of data are kept on every one of us, every day. It is the manner in which those data are used—whether they are used responsibly and whether we have the right protocols to control that use of data—that worries me. That is the main concern.

Q96 Mr David Hanson: You have both exercised the authorisation of intercept warrants, in Northern Ireland and in the Home Office. Could you give the Committee a flavour of how urgent those requests were, how often you turned them down and whether there were any detailed issues—without referring to cases—that you think the Committee would wish to reflect on in relation to the existing authorisation procedure? Perhaps you would like to answer, Lord Blunkett. I can see Mr Paterson passing over to you.

Lord Blunkett: I am happy to do so; I was just trying to share the burden a little. Let us try not to exaggerate. Many of the warrants authorised—there are probably slightly more now than there were in my day, but there were about 2,500 a year—came through on a process of sensible authorisation, which gave time to look at the detail. They were often renewals of authorisation previously given, on a three-month basis, and then more frequently after that.

There were occasions when it was absolutely vital for the services to have an answer in the middle of the night. I am trying not to exaggerate it, because this is not about theatre—it is about reality. On more than one occasion when I had switched off my mobile phone and was not at home, I was literally dragged out of bed by the protection team. When you get one, you have to do it there and then, although in the middle of the night you are not as compos mentis as you might be and you question whether you should pause, drink a coffee and make sense of it. As a whole, it was necessary to be able to turn them around speedily. I know from the questions that Owen has raised in the Commons that both of us are concerned that on critical occasions an incident cannot occur because an authorisation has been delayed.

You asked me a second question: how often did I turn down requests? Out of the numbers we are talking about—I have thought about this a lot—I would say about 2% or 3%. Some of those then came back with further information and clarification that helped me to see that they were necessary.

Mr Owen Paterson: When I arrived at the Northern Ireland Office, it was quite a delicate period. Your Government had just got devolution of policing through. Sadly, there was an element of the republican community that was completely determined not to accept the settlement and wanted to continue physical violence and terrorist actions. They were extremely dangerous. Sadly, we had to ramp up our activity, to get quite a lot of extra money from the Government and to re-equip certain agencies.

I was very aware that we were fighting a 24-hour campaign. One of the first things that I did on day one was to make it very clear to my private office, “This is a priority for me. You wake me and interfere with what I am doing at any time. Never, ever, put my private convenience before speed in bringing one of these requests for a warrant to my attention”.

The vast majority were done in an orderly manner. We had diary slots once or twice a week; I cannot remember how many. As David said, they were frequently repeats. Sadly, it was the same old names coming round and round every three months. As David said, occasionally I would be woken up at 2 or 3 o'clock in the morning and asked for a very urgent decision. That is what has provoked me to make public comments that I am extremely concerned about some of the proposals in the Bill that might interfere with swift executive decision-making.

On the number that I turned down, I am with David. It was a very small number, but I did. It was known that I was not a patsy. I turned down the ones I was not satisfied with, or I sent them back for further information.

Mr David Hanson: That leads to two questions, which both of you can answer. First, how do you now feel about judicial oversight of that process? Is it fair, proportionate and the right thing to do? Secondly, given the concerns that Mr Paterson has raised publicly in the Commons, is there a definition for you of the turnaround time in an urgent case for any judicial oversight commissioner who may be appointed under the Bill?

Lord Blunkett: I am happy with the compromise—I suppose you would describe it as the sophistication—if the process of review is in tandem with the Secretary of State's decision-making process. Historically, judicial review is exactly what it is: a legal and administrative review of the way in which the Executive or their agencies use powers that have been granted to them. In our present process of commissioners, it is down the line when the process is reviewed and checked. This would mean that every decision would be subject to that tandem process. I would be unhappy with it if it cut out the Secretary of State, and those who are vehemently against any kind of intercept and surveillance measures would be horrified if there were not some sort of review now. We are trying to get that in tandem.

Mr David Hanson: It is more approval than review.

Lord Blunkett: That is the debate you are having—to clarify what it is. If it is not a review, are the commissioners being reviewed down the line? There is a presumption in our present political environment that judges know better than anyone else and are better than other people at all sorts of processes. I think that they are very good at interrogating and being able to make judgments in the critical judicial system that we have. I do not think that they are any better or worse than senior politicians at making a judgment on whether the evidence placed before them in these circumstances stands up. If I may be controversial, Chairman, because you have been through it yourself, sometimes you weigh the evidence and use instinct. Instinct is no less valid from those who have come through years and years of the political process and have been publicly scrutinised themselves than it is from judges.

Mr Owen Paterson: I would go further than David. I am wholly in favour of strengthening the review procedure after a decision has been made. Whenever I signed one of these things, I was fully conscious that I was subject to quite a rigorous inspection in the cold light of dawn, possibly some months later. I was fully conscious that I could be summoned to a Committee like this and could be hauled up on the Floor of the House of Commons in Questions. There was a real responsibility. However, I really believe that it is vital that the decision is made rapidly by a Secretary of State with full executive powers of decision-

making. It is up to the Secretary of State to make a decision, often under very imperfect conditions and with imperfect information. As David has just said, often you may have to trust instinct. Our current Home Secretary has done it for five years and is extraordinarily well-placed to make difficult decisions. I wholly fail to see the value of distinguished judges coming in and taking part in the decision. I really oppose it. Go back to Montesquieu and the separation of powers. Their skill is interpreting law or, here, interpreting the manner in which a law has been put into action by an Executive. I feel very strongly that these are executive decisions. They are operational decisions and must be made by a democratically elected Minister, accountable to Members of Parliament.

Mr David Hanson: This is the final question from me. The key element will be the interface between an urgent request to you as the Secretary of State for one or both departments versus a judge reviewing that decision and taking a different view on an urgent case. Where does responsibility lie in the event of that type of conflict?

Mr Owen Paterson: This is what worries me. I stressed in my opening comments that often a swift decision needs to be made. The Secretary of State will be very conscious of his or her responsibility and will make that decision. Here you have a second body party to the decision. Clause 138(3) states, "Where a Judicial Commissioner refuses to approve a decision to issue a warrant under section 137, the Judicial Commissioner must give the Secretary of State written reasons for the refusal"—written reasons. How will that work if the Secretary of State for Northern Ireland is in one place, the commissioners are in another and there is information that may have come from our allies in the Garda Siochána that an operation is under way?

The pass on this has partly been sold. There is the equivalent of an emergency provision, where the commissioners have five days to make a decision. Frankly, that could apply to everything. I would be happy with that. I am perfectly happy to have more judicial scrutiny, more frequent review and more regular meetings with the relevant Secretary of State. They came to see me probably once every six months; you could do that much more frequently. I am very strongly opposed to a member of the judiciary making a co-decision. That is really dangerous. What happens if it goes wrong? Who is to blame? Who comes before Parliament? Who do the relatives sue if a bomb has gone off and a Secretary of State had made a valid decision, under difficult circumstances, with imperfect information, but it had been skittled by a very well-meaning, very well-trained judge on a legal nicety? This has not been thought through. Do they get together in the middle of the night and look at the written review? Do they then together go back to the agency and ask for more information in the middle of the night?

It has not been thought through. I see delay and muddle. There has to be a difficult decision, made by an elected Minister, who is subject to intense scrutiny after the event. This muddles the role of the commissioners. If they are to be a serious body, reviewing and scrutinising, they are compromised if they are active in this decision. It will go one of two ways. Either they will become patsies, to use my earlier phrase, and will just go along with the Secretary of State, so they will be devalued, or they will become an extra body that is not accountable to Parliament. Either of those results is very unsatisfactory. To make it even worse—to get you depressed—it is much worse in Northern Ireland, where you have divisions among judicial bodies, as we saw with the Duffy case collapsing only last month.

Q97 Victoria Atkins: My question has been answered by both of you. The question is, who judges the judges under this format? Please correct me if I am wrong, but there is no accountability for the judicial commissioners, whereas the Home Secretary is accountable to the House of Commons and Select Committees in this place.

Mr Owen Paterson: As I said, I am very concerned that these judicial commissioners will not be accountable. Then there is a third human being with the powers of Solomon, according to the Bill, called the Investigatory Powers Commissioner. If you look at the same clause—Clause 138—subsection (4) states, "Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to issue a warrant, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant". That introduces a third body, with more muddle, more delay and more lack of accountability. I go back to my comments to David Hanson. What happens if it goes wrong? Who is to blame? Who is hauled up before this Committee? Who is hauled up before the Northern Ireland Affairs Committee for letting an operation that could have been stopped go ahead, when the democratically elected Secretary of State had made a clear decision? I am not at all relaxed about these proposals. I really do not like them.

Lord Blunkett: I share Owen Paterson's genuine concern, but I also know, with a political hat on—this is why your Committee has a massive challenge, but why it is sensible to have scrutiny of the Bill in this way—that we need to find a way of ensuring that a tandem process can work, simply because there is an atmosphere now, driven by those who suspect the state of all sorts of things, that makes it very difficult to resile from what has been put forward. Sophisticating it will be the challenge. I would like to wish you luck with that.

Dr Andrew Murrison: Answerability is an important concept, but what does it mean in practice, since Secretaries of State answering on warrantry issues will invariably say, "We do not comment on security matters"? The other point, just for observation, would be the stance taken by the rest of the "Five Eyes" community in relation to judicial oversight, which, even under the Bill as it is currently drafted, is quite different. Do you think that there may be scope for separating warrantry on criminal matters from warrantry on national security matters, removing the Home Secretary from the former?

Lord Blunkett: The problem we have had with authorisation is that the more dangerous the individual or individuals, the more likely it has been that the Secretary of State—or, in the case of criminal behaviour, the Home Secretary—has been dealing with it. We have had almost a perverse situation where the police—obviously you will look at this separately, but I said it in my evidence to the ISC—have been able to get authorisation to do things without going to the Secretary of State. I think that we have it the wrong way round. The Secretary of State should be responsible for the warrantry, for the reasons you are very familiar with. You cannot separate serious crime and the danger of terrorism, not least with interconnection, money laundering and everything that you were debating before we came in.

Dr Andrew Murrison: Would it be a little easier if we had a proper definition of national security, which we do not have on the face of the Bill at the moment?

Lord Blunkett: We have all sorts of articles in relation to exemptions, do we not, within the European Union—I dare not mention it in Owen Paterson's presence—as regards definitions? Earlier Sir David Omand indicated that we have got as near to it as possible, in an imperfect world.

Mr Owen Paterson: Could I add one or two comments? First, I do not entirely agree that Secretaries of State just bat off these questions and say, "It is not appropriate to reply". When serious incidents happen, often there are quite major investigations and what went wrong comes out. This will happen only when something goes horribly wrong, so the process will be exposed.

On the issue of criminal or terrorist issues, I totally agree with David Blunkett. In Northern Ireland, where you cross the line between excessive fuel smuggling, racketeering and drug smuggling feeding violence, which may be criminal or terrorist violence, it is a pretty grey, woolly area. Both those came across my desk, and I did not differentiate.

Q98 **Suella Fernandes:** I have two small questions. You have talked about the notion of instinct that Ministers may have when issuing warrants that the judiciary may not possess and said that it is an important factor to preserve in the decision-making process. Could you say a bit more about what distinguishes the ministerial perspective on such decisions from a judicial approach?

Lord Blunkett: The judicial approach would obviously get there, because after time they would be familiar with the process. That happens to Secretaries of State coming in, but on the whole you do not get people who are inexperienced in the general areas who are Home Secretaries, Foreign Secretaries and Secretaries of State for Northern Ireland. They are still learning when they come in and when they are doing it, as we all are when growing into jobs. I am sure that, after a period of time, those who have been schooled and have undertaken their process of promotion in an entirely different way would come to expect to have to use instinct, but it is not helpful to a judge to use instinct, is it? Judges are not trained to use instinct. They are trained to resist using instinct, are they not, at least theoretically? The facts have to be dealt with, even if the judge believes there is a problem. All I am saying—I am trying to be honest about it—is that you examine the material that has been put before you and do everything that you can to stick to that, rather than what you feel about it, but there are occasions when you think, "I will go with it. My instincts tell me that there is something entirely right about the application and entirely wrong about what these people have been doing".

Suella Fernandes: Would you say that it is a wider perspective, as opposed to a narrower legal perspective?

Lord Blunkett: Inevitably, yes. If it was only a legal matter, you would not have that process at all.

Mr Owen Paterson: That is exactly right. If this was nice, rinky-dinky, clean and tidy, you would not need politicians. You would have these wonderful judges who were all knowing and all knowledgeable, who interpreted law that told them exactly what to do and who did not move an inch off it. If you look at Clause 169(5) and (6), they are expected to make

political judgments. It says, “In exercising functions under this Act, a Judicial Commissioner must not act in a way which is contrary to the public interest or prejudicial to—(a) national security, (b) the prevention or detection of serious crime, or (c) the economic well-being of the United Kingdom”. The judicial commissioner must ensure that he does not “jeopardise the success of an intelligence or security operation or a law enforcement operation … compromise the safety or security of those involved, or … unduly impede the operational effectiveness of an intelligence service, a police force, a government department or Her Majesty’s forces”. Every one of those requires a difficult political decision. There might have been information from Dublin that someone is on the way up. Someone else is coming in from Donegal. You do not have perfect information. You have to trust the information you have been given and you have to make a subjective judgment. You are fully conscious that you might be up for very severe scrutiny—in my case, some months afterwards—in the cold light of day, and you have to make a decision. There is nothing clean, rinky-dinky, nice and tidy that can be delivered to make it easy for a judge. It is absolutely what judges are not trained to do, as David said. It is exactly the opposite.

I am very happy with the five days. I would be very happy with five-day scrutiny and with the Secretary of State being called in every month to meet the commissioner, who would say, “You made this, that or the other decision”, and go over it, but at the critical moment, at 2 or 3 o’clock in the morning, somebody has to make a very difficult decision, and it may be on instinct. In my case, I had been going to Northern Ireland every single week as the Opposition spokesman—as the shadow Secretary—for three years. I had met an awful lot of people, I had been to every corner of Northern Ireland—places where, sadly, I could not even dream of going now—and, in fairness, I learnt a little bit about it. I pulled on that information and on some of the people I had met. David is absolutely right. There is an element of this that is instinct. That is called political judgment. It is not right to put judges in the same box. It is not fair to them.

Suella Fernandes: Where would you draw the line, in striking a balance between national security and transparency in decisions on the issuing of warrants, between judicial and ministerial decision-making power? Would you say that it should be solely for Ministers, with no judicial decision-making power?

Mr Owen Paterson: Yes. I am completely clear. Elected Secretaries of State, accountable to the House of Commons, should make those difficult operational decisions. That will guarantee operational agility and swift reaction. I am all for increasing, extending and making more intense the scrutiny process by distinguished judges, after the event. I mentioned dear old Montesquieu and the separation of powers. It is not a bad thing to go on. He made it absolutely clear that you do not have judges making executive decisions.

Q99 **Bishop of Chester:** The clauses to which you referred are in Part 5 of the Bill, I think, at the end, on bulk interception warrants.

Mr Owen Paterson: Part 8.

Bishop of Chester: Earlier warrants allow a five-day period when urgent decisions can be taken. Is there a particular reason why you think there should be the facility for an urgent decision, not requiring the judicial approval in the later part you have been referring to?

Mr Owen Paterson: I am very happy with the five days. That could be a sensible compromise. The five days allow decision-making by the elected Secretary of State, without interference, without delay, without obfuscation and without muddle.

The Chairman: Can I stop you for a second to clear things up? The five days refer to urgent cases, not ordinary cases. I think that Mr Paterson is saying that, even in ordinary cases, the five days would become a review, rather than a co-decision.

Mr Owen Paterson: Correct. That is exactly right.

Bishop of Chester: There is the practical question of an urgent request, under the later part of the Bill, for the bulk warrants, but there is not provision for an urgent decision. There is in the earlier part of the Bill. You are raising a more fundamental principle as to whether the judges should not operate as they do now, revealing after the event. You are suggesting that that is much better.

Mr Owen Paterson: The Chairman summarised very effectively what I think. The decision should be made by a democratically elected Minister, accountable to the House of Commons. The review should be conducted by distinguished lawyers, days, if necessary, after the event, with the scrutiny process starting at five days. I would be very happy for Secretaries of State to meet the reviewers more regularly.

Bishop of Chester: I understand that that is how DRIPA, the present time-limited Act, operates. There is judicial review after the event.

Mr Owen Paterson: Yes.

Bishop of Chester: That is what you would prefer.

Mr Owen Paterson: There is no judicial co-decision-making. At the moment, judges do not participate in the decision. Under these proposals—it is called the double lock in all the press releases—they will be very actively involved.

Bishop of Chester: To be quite clear, you are striking, in a sense, at the heart of the principle of what is now proposed.

Mr Owen Paterson: Yes. I strongly disapprove of the proposal that judges make executive decisions.

Bishop of Chester: That is what you are saying.

Mr Owen Paterson: Correct; absolutely.

Lord Strasburger: Could you tell us how many times you were held to account by Parliament? Could you also explain why your views, in particular, are the exact opposite of those of our four “Five Eyes” partners?

Mr Owen Paterson: I do not remember ever being called up before any Committee or having it raised in questions in Parliament. I suppose you could say that that is a tribute to the fact that the system works, in that people were careful before putting requests before

me and, I hope, I was also careful in scrupulously reading every detail and not nodding things through. As I said, I did, infrequently, turn them down.

Lord Blunkett: Let us go back. The commissioners reviewed the process and whether we had followed it, within the powers laid down to us, which is what I understand review to be anyway. We also had the annual debate, which, sadly, did not engage the media in the way I had hoped it would. Parliament usually had a robust debate, concentrated mainly not on Northern Ireland but on the Home Office and the Foreign Office, with some thoughtful contributions, but it was not really holding to account in the sense of people understanding and then asking us to explain what we had done in individual cases, for fairly obvious reasons—we were dealing with sensitive material, which we would not be able to explain. That was one of the Catch-22s about reporting back to Parliament when we were debating Bills, including the one that has a sunset clause next year. How can you report to Parliament on detail that is itself subject to the necessary privacy that protects those who have been involved? That is why your job, and the Home Secretary's job, is so difficult.

I fall slightly short of Owen's absolutism on this. I can see entirely where he is coming from, but in the reality of the moment we have to deal with what has been put forward by the Government and the difficulties that they face. I have to be careful here. My second son works for a major company and years ago used to tell me off for being too gung-ho on all this, so I have family problems. Can I be clear? Whatever the Government decide to do, there are people who do not believe that it is either necessary or acceptable. At the moment, they get a bigger hearing than the intelligence agencies.

The Chairman: Could I clarify something Lord Strasburger said? He made an important point. There is no real parliamentary mechanism currently available, is there, for obvious reasons, that could in any way scrutinise the decisions either of you would make on agreeing intercept warrants—even to the extent, I guess, that the ISC, meeting in private, would not be able to deal with them?

Lord Blunkett: I see no reason why we should not have a much more thoroughgoing report on the number of decisions taken and the nature of those decisions. When the then Foreign Secretary, William Hague, reported to Parliament on the back of what happened with Snowden, I said that we could be a lot less diffident and sheepish about all this, without putting the intelligence and security services and their operatives at risk. We should examine how we might do it more openly. We could also examine areas that are outwith what the Bill is able to deliver, namely where information is provided from other agencies outside this country and there has been no warrant and no clearance. The information is given to us, and we have still not come to terms with that.

Lord Strasburger: You seem to be confirming the view that the concept of parliamentary scrutiny of warrants is a myth.

Lord Blunkett: I do not know anyone who has really believed that Parliament scrutinises the warrants system.

Lord Strasburger: Exactly.

Lord Blunkett: The commissioners have. They produce their annual reports, which are usually commented on in the media, but Parliament, other than in the annual debate, does not and has not.

Lord Strasburger: But both of you gentlemen, particularly Mr Paterson, have waxed lyrical about the concept of parliamentary scrutiny. I am struggling to see where it is.

Lord Blunkett: No. The politician is accountable. That is different from the way in which Parliament chooses to scrutinise or not to scrutinise. Secretaries of State are accountable, both publicly and to Parliament, and can be sacked. I wonder under what conditions a judiciary involvement would result in their being removed.

Mr Owen Paterson: That is the key point: we are accountable. There is a lot of information about decisions made by Secretaries of State. Ultimately, those decisions can be taken up by parliamentarians, should they choose to do so. As David said, at the moment there is only a debate. Should things go wrong, Secretaries of State can absolutely be on the line and accountable to Parliament.

Lord Strasburger: As far as I know, it is not legal for a Secretary of State to discuss a warrant in public.

Mr Owen Paterson: But a Secretary of State is accountable to Parliament for activities in his or her sphere of influence—and can be fired.

Victoria Atkins: I can help Lord Strasburger. Sections 17 to 19 of RIPA make it a criminal offence for Secretaries of State to answer questions on this, if they are so asked. That may help to answer his question.

The Chairman: You have been let off the hook today.

Lord Blunkett: That never passed across my consciousness when I was there.

The Chairman: I move now to Lord Henley, because Mr Warman's questions have been answered.

Q100 Lord Henley: I want to come on to the various safeguards for privileged communications. You will remember the statement that was made by the Home Secretary on 4 November and the concerns raised by David Davis, in particular, about the lack of protection that MPs have over the potential acquisition of their communications data. Does the enshrining of the Wilson doctrine in statute provide adequate protection for legislators' communications and address the concerns put forward by David Davis, or should there be additional safeguards over the use of communications data for parliamentarians, as there are for journalists?

Lord Blunkett: It may be worth cross-referencing briefly to the inquiry that took place after the incursion into the Palace of Westminster in the Damian Green affair. That was old-fashioned taking away of materials, as opposed to intercepting them through new, modern information, communications and Internet provisions, but the principles were the same. That Committee, on which I served, was under the chairmanship of Ming Campbell, now

Lord Campbell. It is worth testing it out. If we are honest about it, the Wilson doctrine was more in intention than it was in reality. How carefully can I put this? What you are doing in this improved Bill is what we were trying to do. My predecessor, Jack Straw, brought in RIPA, and I had the undoubted "privilege" of implementing it. The intention was to be helpful, although people have interpreted it entirely differently since. On the Wilson doctrine, we should distinguish what is privilege in terms of protecting Owen Paterson's electors—my previous electors—from the issue of protecting the parliamentarian. Over to you, Owen.

Mr Owen Paterson: That is a good way of putting it. The principle of privilege, not the individual, is the key point. My main concerns with the Bill are to do with warrantry and powers of decision-making. When it came out, I read it and saw the statement that any proposal involving an MP or any other elected body—the Scottish Parliament, Welsh Assembly et cetera—has to go to the Prime Minister. There has to be an element of common sense. To go back to Suella Fernandes's question, it is a bit of instinct; anyone who thinks of putting any marker down on an MP has to think really carefully in advance. Common sense will probably be the best defence.

The Chairman: That was another very interesting, riveting session. We are very grateful to you both, because it has come from a totally different perspective from that of our earlier witnesses and gives another interesting aspect to our deliberations. No one can say that both of you have not put your views with great robustness. Thank you very much for coming along.

Mark Hughes, President, BT Security (QQ 101-115)

Evidence heard in public Questions 101-115

Oral Evidence

Taken before the Joint Committee

on Wednesday 9 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Lord Henley, Lord Strasburger.

Witness: **Mark Hughes**, President, BT Security, gave evidence.

Q101 The Chairman: A warm welcome to the three of you. Thank you so much for coming along. You represent very significant companies with a lot of relevance for this particular Bill. Apologies to you for starting a bit later, but there was a vote in the House of Commons, which delayed our procedure. I am going to kick off the questions by asking you all to answer the one I am going to ask. If you want to say anything by way of a short general statement, perhaps you would like the opportunity so to do when I have asked the question. Again, welcome to you.

My question is a fairly simple one: how extensively is the Home Office engaged with you with respect to the provisions in the Bill? Perhaps Mr Hughes would start.

Mark Hughes: We have been consulted. We welcome the consultation that we have had. We have had a number of opportunities, and, overall, we are pleased with the level of consultation. There are obviously circumstances where it could be better and we could have done more, but, broadly speaking, it is very different from previous iterations we have had with the Home Office so we are comfortable with the consultation that we have had.

The Chairman: Thank you very much. Mr Kinsley.

Adam Kinsley: Indeed. I would echo that. There has been extensive consultation over the last months and it has been a marked improvement on last time.

The Chairman: Good. Finally, Mr Woolford.

Hugh Woolford: I would echo that. We have had engagement, and we have had high-level engagement both on the legal and operational sides. It is welcome that we are having that engagement.

The Chairman: That is a good start. Lord Butler.

Q102 Lord Butler of Brockwell: Following on from that, you are satisfied with the consultation, but has it led to agreement about what is practicable? Let me elaborate on that while you are thinking about it. This is on the nitty-gritty of how it is done. I am after whether

you think it is practicable to separate communications data from content, or at least the type of communications data you are being asked to retain, whether you are confident that you have the equipment that would enable you to do that, and whether you can give us some idea of what degree of extra costs that would impose on you. I hope that is not too much of a question.

Hugh Woolford: I will kick off and then pass across to my colleagues. I will take it in bits. On how easy it is to separate communications data from content, in the dealings we have had to date we feel that we need more work to get more clarity over what is considered content versus communications data. We need more workshops between the bodies to flesh that out. At the moment there are very high level—

Lord Butler of Brockwell: Excuse me, but does "bodies" mean the Home Office and the providers?

Hugh Woolford: Absolutely, yes. At the moment there are very high-level definitions. You could, for example, say that a route URL for bbc.co.uk is considered communications data, but if you put a "/news" on the end that may be content, so there are nuances—this is the way the Internet is constructed and used—that mean that does not always hold true. There are some general principles in place. We need to move forward and get some more detail in place around some of those nuances and how to handle some of them. That is the first point.

Leading on from that, given that we have not got to the nub of how we would differentiate, the answer is no, to be perfectly honest. We have early discussions going on with regard to some of the equipment or angles that we could look at, but there is a huge piece on volumes, which I am sure we will come to later in the session, that has a massive bearing on the equipment that we need and therefore also the cost.

Adam Kinsley: At this stage, we have to differentiate the conversations and the factsheets we have seen and what we are looking at in the draft Bill. The draft Bill is obviously very high level and it is not sufficient to be able to map across from that and understand exactly what we are going to need to do. By definition, it is going to have to come later in codes of practice and in further discussions. Going back to your question, to be able to differentiate and look at communications data within what are effectively packets of data, there will need to be investment in new types of technology for us to be able to get up to the first slash. The way the Internet is arranged and operated is not simple. We are going to have to look at individual use cases and understand exactly what we will need to do. Hopefully, that answers your question.

Mark Hughes: There are a number of parts to the question. The first is whether or not it is technically feasible to separate content from communications data. The draft Bill usefully defines communications data both from an entity and an event point of view, which is a new set of definitions, as opposed to the previous or existing regime—the RIPA regime—and then content. Technically, it is feasible to separate various parts of the packets; we can deploy tools to do that. The point about that is that, increasingly, especially in the future, with more and more encryption, the ability becomes more limited to take you back to purely an entity level piece of communications data as opposed to richer parts of communication data. That is the first thing.

More broadly, there is a lot of discussion, and has been, about definitions. We have already started talking about them today. It is important to look at definitions in the context of the level of intrusiveness that is the purpose behind the power being sought. That is always the reference point. The definition comes from the level of intrusiveness that is going to impact on our customers and on citizens generally. The definitions are derived from the level of intrusiveness to help bucket, effectively, certain types of data, be it first slash-type data or whatever it may be, to have a way of defining certain types of data. The caution I always put on definitions is that it is not easy to write them down, and we can see that right across the Bill, but with the additional checks and balances put into the draft Bill around legal oversight stuff, there is the possibility to refer back to the level of intrusiveness. Where the definition in the draft Bill might not be sufficient at the moment, there is the possibility through oversight to question that.

I think your next point was about whether or not the equipment exists. Yes, it does. There are various technologies available to us, although they are limited by the way in which the traffic is sampled, and there are many considerations around that. Indeed, some of the Bill, especially in the area of Internet connection records, which are new data that we have never collected before for that purpose, means that we will have to deploy new equipment to comply with the legislation as it is drafted. That comes at a cost. Clearly, there are two things about costs that concern us. First, it is not clear in the Bill at the moment that we will be eligible to recover all our costs, and we think that is important for two reasons. First, the mere fact of defining how much something will cost to meet a certain type of power will help to limit and frame the level of intrusiveness. In other words, an open-ended view of what something could cost could be problematic in the sense that capability could be stood up, which could cost a lot. Therefore, a proportionality check comes in through ensuring that it is clear that costs will have to be met. Secondly, clearly, if the cost is not met in that way, it will have to be found in some other way. There will be additional costs and we certainly have some views on some of the calculations—perhaps we might talk about that later on.

Lord Butler of Brockwell: When agreement on definition is reached, how do you envisage that it will be expressed in statutory form, or would it be expressed in statutory form? Would it be by a statutory instrument or will further amendments to the Bill be necessary?

Mark Hughes: This process, through scrutiny, is in part helping to tidy it up. There is, I believe, much more work to be done to ensure that we get tighter definitions where we can. Equally, as in my previous point, we have to ensure that the oversight regime allows us the ability to discuss that. More specifically, to answer your question, the codes of practice, which we look to see before the publication of the final Bill, will go some way to clarifying a lot, as well as the oversight instruments that exist in the draft legislation, which will allow us, if we are not comfortable with that, to visit it with the appropriate authority.

Q103 Lord Strasburger: Gentlemen, you have mentioned encryption as being a complicating factor. We have also heard in previous sessions that the way the Internet is increasingly being used—for example, with a Facebook page—is as a smorgasbord of content and data, and that it may be impossible to separate them automatically. I doubt that you would fancy doing it manually. How are you going to cope with that problem?

Adam Kinsley: You have put your finger on the nub of the technology challenge. When you are requesting a page within Facebook, facebook.com/spurs, or something like that, you are going to get lots of different content delivered: you are going to get the league table, the Harry Kane goal or something like that—lots of data. We need technology to analyse all of that, match it all up and work out which bit is the first slash. It is a big technology challenge. As Mark says, it is not impossible but it is very expensive.

Lord Strasburger: Thank you.

Q104 **Dr Andrew Murrison:** Obviously, there is some urgency to all this because the Home Office would rather like to get cracking with gathering the information that it says is necessary to safeguard security and deal with serious crime. I am interested to know from you how long you think it is going to take, given the technological challenges that you pose, to get to that first slash point.

Hugh Woolford: We have put some thought into the timescales. As long as the necessary discussions and detail were worked through, we feel that we could probably start in 2017, with earliest deployments in 2018, depending on the requests and the scale. Those are the sorts of timescales that we would potentially be working to.

Dr Andrew Murrison: That sounds quite a long timeframe to me. Does that match the level of patience that you perceive in your dealings with the Home Office, or is it disappointed by that?

Hugh Woolford: I honestly cannot comment on that. Those are the timescales that we have in mind. That is currently where our heads are.

Dr Andrew Murrison: I have to say that the definitions on the face of the Bill confuse me; I suspect that they will probably be rather clearer to you since you are in this particular business. I have heard from you already that you value the improved definitions, particularly those in Clause 193, which I guess is what you are referring to when talking about entity data and events data, but I am also hearing that you expect further clarification by way of codes of practice. Where do you think we are at the moment with the definitions? Where on a Likert scale of zero to 10—where zero is completely useless and 10 is perfection—do you think we are at the moment?

Adam Kinsley: I am not sure that the intention is for us to be able to deliver any capability based on the face of the Bill alone. As it stands, it is pretty close to zero, I would say. We absolutely need more detail to be able to deliver. I am not sure it was the Home Office's intention to be able to deliver based on the definitions on the face of the Bill, but that is obviously a decision for Parliament—how much goes on the face of the Bill, how much goes into codes of conduct.

Mark Hughes: There has been a lot of work to help to clarify a number of the definitions in the Bill. In the Internet connection records space, for example, it is difficult for us to comment because we are not defining the purpose for which it is intended. Therefore, by its very nature, I am not in a position to comment. There has been a lot of work. As we have already said, there needs to be more work and the codes of practice should support that.

Adam Kinsley: I should qualify my comments. I was answering in relation to Internet connection records primarily.

Hugh Woolford: I would echo that.

Q105 **Mr David Hanson:** Page 25 of the draft Bill, regarding Internet connection records, says helpfully: "A kind of communications data, an ICR is a record of the Internet services a specific devices has connected to, such as a website or an instant messaging application. It is captured by the company providing access to the Internet". Is that your understanding of what an Internet connection record is?

Hugh Woolford: Today we do not have anything like an Internet connection record. This is something that is completely new for us, and I have looked at previous Bills. From a business point of view, there is no need for us to capture any of this information. We do not have what could be classed as an Internet connection record.

Mr David Hanson: I am a layman here, so tell me how hard it is to collect one of those, to establish it.

Mark Hughes: On the face of it, it sounds like a relatively straightforward thing to do. In some respects, the Bill goes on to define the purposes for which they are being collected, and three purposes are outlined. They are obviously around the person, illegal content and the service, broadly speaking. It helps as well when you combine the two things; you take the initial definition and the purposes that are in the draft Bill, and that has given us a route to analyse what would need to be collected—as Hugh said, it is not something that we collect today—to fulfil that definition and then have data available if that were to be the case for that purpose. You would have to look at quite a lot of data to be able to achieve that.

Adam Kinsley: If you think about what a CSP would be required to retain at the moment, essentially you may be given an IP address that would be applicable to your computer for potentially up to a week and that would get recorded once. There are a couple of bits of data that would be recorded for about a week. In what the Bill is seeking to do, first of all you would have to analyse all your Internet sessions in that week—in fact, throughout the whole year—which would obviously be quite a lot; in the Facebook example we used earlier, just one request to a Facebook page will come back with lots of information within it that needs to be matched. You need to analyse all that, match it all up and then retain the bit that the Bill will ultimately end up with. The magnitude of data collected that would be processed would be massively more and the magnitude of data that would then be retained would be tenfold, a hundredfold more than we collect today.

Q106 **Mr David Hanson:** At the moment we are considering the draft Bill; it is going to go through the House of Commons and the House of Lords and be law by September or October next year. How long is it going to take you to establish the mechanisms? How much is it going to cost you to establish the mechanisms? Who do you think is going to pay for this? Is it the taxpayer, as in all of us? Is it you or a mixture of both? If so, what is the mixture? Is it practicable? Is it going to do what it says on the tin? We need to get a flavour of this from you.

Mark Hughes: Let me go through a number of those things. There is a spectrum of options available on Internet connection records in terms of the amount of coverage. The Home

Office has consulted us and we have had a pamphlet that has been issued about Internet connection records, with some view of costings. We have obviously done work based on the assumptions. The assumptions from the Home Office are that it wants as broad a coverage as possible to achieve this, which is going to be costly. We have worked up some assumptions and indicative costing.

Mr David Hanson: Are you able to share that with us or not?

Mark Hughes: Yes. The publicly stated figure, I think, from the Home Office is that it has set aside £174 million for this. We have worked out that for us alone—I cannot comment for others around the table or others in the industry—to fulfil the assumptions that we have been given will cost us tens of millions, so the lion's share of that £174 million would be for us alone. How others would do it depends on how they manage and architect their networks. We have looked at it. As to the implementation time that it would take, again it depends: there are some things where extant capability could be used to gain some coverage relatively quickly, but to fulfil the assumptions we have been in dialogue with the Home Office on, it would take longer to deploy equipment comprehensively across our network—deep packet inspection equipment—to be able to generate the data to then have them retained to comply with the legislation.

Hugh Woolford: On costs, we broadly agree. Our teams have had a look at the high-level information we have and think similarly—tens of millions. I would love to give you an exact figure. We are not saying it cannot be done. Anything can be done in this space with enough time and money. We have a broad set of requirements, but to enable us to move forward we need to bring some more specificity to those so that we can start giving more accurate estimations of costs and time. Depending on how much you are trying to capture and across what frequency, one big piece of it is how much of whatever the equipment is you might need to deploy; therefore, you need to find space, power and places to host it all. It is no mean feat. This Bill potentially could look at all of us having almost to mirror our entire network's traffic to enable us to filter it. It is a huge undertaking.

Mark Hughes: You asked about costs. We believe quite strongly that the costs should be met by the Home Office—that we should seek to have 100% of our costs in this space reimbursed. The reason is that, if you start from the basis that there is no cap on the cost, you may end up with a disproportionate technical solution that could be overintrusive, so the cost in itself will help bound the solutions.

Mr David Hanson: To help the laymen and women among us, if the taxpayer chose to support the cost of developing this scheme, do you think £170 million is a reasonable estimate, given what you have said in your previous answers, or not?

Mark Hughes: Based upon the assumptions we have seen, from our point of view, yes, because it would cover what we need to do, but if you aggregate it across the industry—

Mr David Hanson: It is not just you, is it?

Mark Hughes: Absolutely not.

Mr David Hanson: Otherwise the terrorists and criminals would not use BT; they would be using something else, would they not? So it cannot just be you.

Mark Hughes: Indeed. There are obviously other ways in which other networks are architected. There are, though, other assumptions. You could use less sampling of traffic, which would perhaps give less coverage, but there would be a trade-off in the amount of cost.

Q107 **Mr David Hanson:** This is the final question from me, Lord Chairman. Let us look two or three years ahead to when this has all been done, someone has paid for it, it is all available and the aspirations on page 25—of the Government and you—have been met. What do you think about how the Government access that material? Are there sufficient safeguards in the Bill for single point of contact officers? Are there sufficient safeguards in the Bill for access by the security and police forces via the Home Secretary, or whoever, in the Bill?

Mark Hughes: On that point, the Bill is clear that there are three purposes under which the data we are talking about, the Internet connection records, can be disclosed. That is fine. However, there are further parts of the Bill that refer to forward-looking capability. We believe, going back to one of the points I made earlier, that that potentially changes the intrusiveness before the data are disclosed and would, in our view, require a check against the level of intrusiveness that it would incur and a referral back to the legal oversight to ensure that we were not stepping outside the intention that was originally conceived in the three purposes.

Hugh Woolford: Can I raise an item on the emergency single point of contact? One of the items that is suggested is emergency SPOCs. We feel that could give rise to an ability to breach the system. In an hour of need—the golden hour—how are you going to validate who is asking for the information? It would be better if the normal SPOCs—if "normal" is the right word—were to provide cover so that there was a single list of authorised people who can ask for it. Having an emergency, somebody ringing up or contacting and saying, "We need this because someone's life is in danger", gives an opportunity for that to be abused. We feel it is better if the SPOCs cover each other. That is an area that we would like to have looked at.

Mr David Hanson: Apart from that, it is all going well.

Q108 **Stuart C McDonald:** I have one short supplementary on these points. One or two witnesses made reference to a similar scheme that was operated in Denmark. Is that something you guys have looked at? What were the similarities and differences? Is there anything that can be learnt from what happened there?

Hugh Woolford: No, I have not looked at that, I am afraid.

Mark Hughes: I understand that the system in Denmark has failed because the software has not worked. That is what I am led to believe.

Stuart C McDonald: Is there anything we can learn from that? Is the scheme that you are being asked to implement similar?

Mark Hughes: I am not familiar with the ins and outs of the detail of it; I am just aware of the headline. Through the consultation and the technical feasibility that we have done, we believe there are technical solutions that we can put in place—subject to the Technical Advisory Board confirming that. They would perhaps draw on that Danish experience, but we have to be careful that we implement them properly. There is no reason why, if we have the right solution and we implement it properly, it will not work.

Q109 **Lord Butler of Brockwell:** I have one supplementary. Could you break down the £174 million between the one-off cost of getting the right equipment and then the recurrent cost of maintaining it?

Mark Hughes: The capital investment—the deep packet inspection-type equipment that needs to be put in place—has to be factored against the very strong growth, or fast growth, in bandwidth over the period. The Home Office looked at this over 10 years. Then there is obviously the ongoing cost of maintenance, but also primarily storage. There is an initial upfront investment, but storage is the thing that is going to take up a fairly big chunk of that cost.

Lord Butler of Brockwell: Can you give us an indication of how much of the figure you gave is the once-and-for-all cost?

Mark Hughes: I do not have the figures off the top of my head, but it is skewed quite heavily towards making sure that there is storage. It is not to say that the initial investment is not insignificant, but the storage is also a significant part of it.

Lord Butler of Brockwell: We are talking about £174 million per year, are we?

Mark Hughes: No. From my own point of view—BT's point of view—it is a fraction, so to speak, of that, but we look at it over a time period. There is an initial upfront investment and thereafter the storage.

Adam Kinsley: It is possibly worth adding that, whereas in the previous regime data growth did not matter that much, in this regime it very much would and data growth is running at doubling every 18 months or so. That needs to be factored into any equation.

Q110 **Suella Fernandes:** It will be a challenge to maintain the security, but to assess the challenge that is going to be presented by the Bill, what in a technical capacity is available to you to reassure the public on the security of data retention?

Hugh Woolford: We have discussed this. We will obviously look to work with the government security advisers to ensure that any processes and systems that we put in place to meet this Bill would meet those requirements and then regular auditing of them. That is the best way we think we could assure that everything was secure and in place. As a matter of course, you have to create a culture and a process around it that brings rigour.

Suella Fernandes: What is your assessment of the effectiveness of things like firewalls and personal vetting systems, and how realistic are they as tools to expand on?

Mark Hughes: It is about creating a layered approach to defence, ensuring that the controls are proportionate, given the sensitivity of the data. We are talking about collecting data for the first time—data we have not collected before—and the key is to ensure that our customers and their rights are protected. That data has to be looked after very carefully, so we have to have a commensurate security wrap around them that takes account of our customers' human rights and indeed their privacy as well so that we ensure that we maintain and safeguard that.

Adam Kinsley: We currently work with the Government on standards, but it could benefit from being more joined up on the Government's side. The Home Office, the ICO and the National Technical Assistance Centre having a single set of standards that we could build to would make a lot of sense.

Mark Hughes: We see a key role for the proposed Investigatory Powers Commissioner and its office being responsible. Clearly the Information Commissioner's Office has a role as well, but it would be useful to us in this context to have a joint agreement between the Investigatory Powers Commissioner and the Information Commissioner's Office, perhaps through a memorandum of understanding. We would rather have the Investigatory Powers Commissioner as the authority to which we could go to seek advice to ensure that we were meeting the correct standards to safeguard that information.

Suella Fernandes: Of course the Information Commissioner will have an auditing power over the security of the systems. How would you describe the appropriate level of engagement with the Information Commissioner?

Adam Kinsley: In the past we obviously had normal business interaction with the Information Commissioner. It seems to us that with this opportunity, when we are creating a new commissioner for these purposes, it might make more sense to bring all of that under one roof; if we are looking at the security of these specific systems, now might be the time to look at having it all under the Investigatory Powers Commissioner rather than two separate organisations.

Hugh Woolford: We absolutely echo that. It brings clarity and conciseness. That is our absolute view. We would rather have it brought under one, definitely.

Q111 Suella Fernandes: This is my last question. There is some suggestion of introducing a criminal offence for data breach by communication service providers. Do you think that is going too far? Do you think it could act as an incentive?

Mark Hughes: We take the privacy and security of our customers' data extremely seriously. As is well reported in many parts of the press, it is something that we take so seriously that we do not necessarily see criminal powers as necessary. We already take it extremely seriously and we believe that the sanction if something goes wrong is that one can quite clearly see the consequences almost on a daily basis.

Hugh Woolford: That is more or less what I was going to say.

Q112 Stuart C McDonald: I want to ask about request filters. What is your understanding of how a request filter would work, and what concerns, if any, do you have regarding its operation?

Hugh Woolford: We have had engagement on the request filter. It is not specified as such in the draft of the Bill. We understand that information would be asked for, we would pass it into a filter and then ensure that only the specific information is passed back, so it stops massive information coming back. We have a few specifics, but the principle is purely at high level, as a concept more than anything else, at the moment. Without wishing to sound like a broken record, this is something else that definitely needs to be looked at and worked through in more detail. One thing that we do not want to do is to become data analysers of information.

Mark Hughes: We understand that it is for the Home Office to design and build the request filter and that it will sit between us as a communication service provider and the law enforcement agency. That is how we see that it will work, but, as Hugh said, there is more to be done. It will use an algorithm essentially to limit the data that are disclosed or presented to the law enforcement officer, who is obviously authorised to see the data, so it limits the data just to those who are necessary to that question.

Stuart C McDonald: Does the information you have just given arise from discussions you have had with the Home Office?

Mark Hughes: It is what I understand from discussions we have had with the Home Office. We have a concern, once the system is effective and in place, that there could be a situation where lots of questions are asked and continue to be asked of it, so our view is that more work needs to be done through consultation to ensure that we—again, going back to my previous point about intrusiveness—level up if multiple questions lead to a point where it is becoming overintrusive. An important principle for us throughout the Bill is that we should always level up to the highest level of authority when we think intrusiveness is becoming greater than was originally intended.

Lord Strasburger: There is a view abroad that the provision in the draft Bill for the request filter is not much more than a placeholder for the Home Office to return to this in the fullness of time and, effectively, write its own cheque on what this will deliver. From what you are saying, it is not giving you very much detail about what this is to do. Is that a possibility?

Adam Kinsley: I would not like to comment on whether it is a possibility. As I understand it, the request filter is there to limit and to be a protection against the flows of information. I would not want to speculate where it might go. We certainly have not seen—

Lord Strasburger: The fact is we do not know where it is going.

Adam Kinsley: The fact is we have read factsheets and had discussions about the concept.

Mark Hughes: The thrust of it is that it is about limiting the amount of data that will ultimately be disclosed to answer a particular question, which is important from a proportionality point of view.

Q113 Lord Henley: Can I turn to the maintenance of technical capability and what is proposed in Clause 189 of the Bill, which you will be aware of? As you know, the Secretary of State will be able to impose various obligations on relevant operators and that will take the form of a technical capability notice, and she will obviously have to consult about that. What are your views on the ability of the Secretary of State to impose a technical capability notice? How do you think your customers are going to react if they are aware that the power exists but they will not be aware of any specific imposition, because that will not be disclosed?

Mark Hughes: There are a few points on technical capability notices. The first one is that we believe quite strongly that the Bill should be clearer in its definition of the fact that the capability notice should be limited to public telecommunications services. At the moment, the definition is not clear, and we are quite clear that it should not extend to private services; it should be limited specifically to public telecommunications services. The second point is that the notice should be served on the provider who is closest to where the information can be provided from. You used the example of Facebook earlier on. That is a matter for Facebook to deal with and the technical capability notice should be directed at that organisation, if indeed it is the closest to the information, which is its information. It should be served, therefore, on those closest to the place where the information is maintained. Beyond that, the existence of a technical capability notice, as in the draft Bill, formulated through the Technical Advisory Board, is good. That there is consultation and oversight that needs to happen before it can be issued is a positive thing.

Lord Henley: What about the views of your customers?

Hugh Woolford: It is definitely not my place to comment on what the views of our customers may or may not be, I am afraid. We are concerned about that, absolutely, but at the moment we have not consulted with them or asked them, so it is wrong for me to offer up an opinion.

Mark Hughes: It is not the technical capability notice per se; in entirety, all the notices that come from this, those beyond the technical capability notices, are something that our customers need to be aware of. Transparency is one of the reasons for this new Bill.

Q114 Lord Henley: You mentioned oversight and the importance of that, and it was partly dealt with in earlier questions from Ms Fernandes about the Information Commissioner. I forget who answered this and whether it is your collective view, but I got the impression that you would like the proposed Investigatory Powers Commissioner and the Information Commissioner to be one—to be merged.

Hugh Woolford: Yes.

Mark Hughes: I am not advocating a merger, but for the purposes of the Bill we feel that for the Investigatory Powers Commissioner there should perhaps be some memorandum of understanding with the Information Commissioner. As I understand it, the Information Commissioner has many other jobs to do beyond this. There is no merging of the two, but just for the purposes of this Bill it would be useful to have one place to go to. We are all agreed that it is the Investigatory Powers Commissioner.

Lord Henley: Because the Information Commissioner is doing other things, in other words, he would delegate his bit of it.

Adam Kinsley: I am not sure how you would bring it into effect. If what we are talking about is security oversight of systems designed to fulfil the obligations in the Bill, it seems that the specialist commissioner would be best placed to carry out that function.

Mark Hughes: Can I make one more point about the technical capability notice? Following on from the point about those providing the service, and that the one closest to the service should be the focus of the Bill or any action that is served, it is not appropriate, we believe, for a network provider to be used as a one-stop shop. It is absolutely important that we process and manage data on behalf of our customers. Where that data is processed by another organisation, it should be subject to the technical capability notices.

Hugh Woolford: Adding to that, if I may, the retention and storage of third-party data is something we are also concerned about, linked with that whole piece. We do not want to be seen as that one-stop shop and asked to retain and store data for third parties that are not to do with our core business or core customer groups.

Lord Strasburger: How do you feel about GCHQ engaging in covert bulk network interference against your networks?

Adam Kinsley: I personally do not have a view on that. That is a matter for you guys to consider.

Q115 **Lord Strasburger:** My question is: how do you feel about your networks being amended covertly by GCHQ and the risks associated with that?

Mark Hughes: It is important to note that any power in the Bill that is instigated in that particular arena has to be proportionate and has to have the right checks and balances over the amount of intrusiveness. The oversight has to take account of the fact that, by their very nature, those types of powers are quite intrusive, so the levelling-up process of the oversight needs to be such that there is full legal oversight.

Lord Strasburger: My question was about the risk to your networks. That is what I was asking about.

Mark Hughes: We are certainly not in favour of anything that would undermine the integrity of our networks.

The Chairman: Gentlemen, we are very grateful to all three of you. Thank you very much for coming along and giving evidence to us.

Professor Bill Buchanan, Head, Centre for Distributed Computing, Networks and Security, Edinburgh Napier University (QQ 207-215)

Evidence heard in public Questions 207-215

Oral Evidence

Taken before the Joint Committee

on Monday 21 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Suella Fernandes MP, David Hanson MP, Shabana Mahmood MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Lord Hart of Chilton, and Lord Strasburger.

Witness: **Professor Bill Buchanan**, Head, Centre for Distributed Computing, Networks and Security, Edinburgh Napier University, gave evidence.

Q207 **The Chairman**: A very warm welcome to all three of you. Particularly as we are so close to Christmas, it is very good of you to come along and give us the benefits of what I know is your considerable expertise, knowledge and experience. We very much look forward to listening to you. I will start by asking you a general question, which will give you the opportunity, if you so wish, to make any general statements about the Bill. Will it work? What are your views on the draft Bill from a technical standpoint and are these proposed powers workable? Perhaps we will start with Professor Buchanan.

Professor Bill Buchanan: Thank you. I would say that we live in a very different world from the one that we did. We have built this cyberage within about 40 years, but the infrastructure that we have created is very fragile. We must protect citizens from hackers and so on. We must protect privacy and identity. More and more services are moving towards the provision of both privacy and identity. Individuals need to be assured that they are not being spied on by cybercriminals across the world. They also need to be able to prove their own identity and the identity of what they are connecting to.

Encryption involves both these aspects. It keeps things private but it increasingly is also used for identity provision. Much of cryptography is now focused on proving the identity of the services that we connect to. Just now, most of the services that we use in the cloud—Google, Amazon, Facebook and so on—are encrypted. Every time we see "https" and we see a green bar on our browser, it means that we are protected with a unique cryptography key for every session that we create. It is almost impossible to crack that key without knowing the private key of the site to which we are connected. The only way that someone could crack communications through a tunnel such as that is to get the private key off the company that is involved in the communications, which would involve Microsoft, Facebook, Twitter and so on handing over their private keys. The problem around that is that if someone gets access to those private keys—those special keys—we open up the whole of the internet and we will have the largest data breach that has ever been caused.

The communications that we have are obviously highly sensitive. The logs that we see on the internet are really the history of our whole lives. They are our thoughts, beliefs and dreams almost by the second. Every single thing that we do is recorded in our web history. The amount of money that that would be worth to a criminal—a cyberhacker on the internet—would be almost unlimited. If an ISP was hacked, you can imagine what the logs could be used for and what bribery there could be for individuals and companies. A balance needs to be struck between the privacy of individuals, the protection of our businesses and the risk of serious organised crime.

Erka Koivunen: Lord Chairman, it is an honour to be present in this Committee session. It has been a fascinating journey to read through the Bill, in particular as a non-native speaker—it has been a tedious task. However, I would like to offer my congratulations. The Bill is pretty transparent in the way in which it lays out the intentions of the Government to do a lot in terms of law enforcement and signals intelligence. This is a Bill that you would get if you asked signals intelligence organisations what they would like as a Christmas present; they would reply that they wanted this and wanted it in bulk.

However, there are some unintended consequences when writing broad legislation that would give such exceptional powers to intelligence agencies and law enforcement. If there ever was a question whether nation states, Governments and military organisations would be engaging in hacking and computer intrusions, I guess that this Bill solidly sates that, yes, this is what they do and this is what the UK Government are actively seeking to do. Frankly, this is something that has been going on for quite a while now. The Bill is an attempt to put the existing situation in writing. We, as a provider of cybersecurity services to private companies and Governments, would typically advise our customers to be aware of criminal activity taking place and of their organisations being targeted by nation states and Governments as well. No better marketing material for services such as those that we provide could be envisaged. We should be aware that the powers laid out in the Bill could be misused. This will lead other nation states to try to mimic these powers. As a member of the European Union—I come from Finland, I am a Finnish national and our company comes from Finland—I feel that I am now a target of many of the activities laid out in the Bill. I do not think that this is what I signed up to when I joined up the cybersecurity profession. There are lots of discussions on how to limit those powers. I am not a lawyer or a legal person, but there are lots of things I can imagine technically that would undermine our society's security. Some of the things that we build in our online systems depend on strong cryptography, in terms of encryption, authentication and authenticity.

The Chairman: Thank you so much indeed. It is very good in English and in Finnish. Mr King?

Eric King: I will not repeat any of the feelings and concerns that both Bill and Erka have highlighted, but perhaps I can help the Committee in one regard by focusing your minds not on the question of whether the proposed powers are necessarily workable, because the majority of them are in fact already in use. That is not to say that they are powers granted by Parliament—indeed, I would expressly say that that is not the case—but they are powers that our agencies have been deploying for a number of years.

It has only been this year for the most part that the public have found out about these and that they have been officially avowed. It was in February this year that the Government avowed hacking for the first time—it is now called "equipment interference". In the

Investigatory Powers Tribunal a few weeks ago, I heard from government lawyers that bulk equipment interference apparently had still not been avowed. Bulk interception was only avowed with the writing of the ISC's report in March this year, for which we are very grateful. The use of bulk personal data sets, as mentioned in the Bill, were again revealed to the public only with the ISC's report in March. The ISC stated at the time: "Until the publication of this Report, the capability was not publicly acknowledged, and there had been no public or Parliamentary consideration". Bulk communications data acquisition was only avowed on the very day that this Bill was introduced to Parliament by the Home Secretary, who admitted that our Security Service, MI5, had been acquiring in bulk the phone records of everyone in the United Kingdom. Anderson commented at the time to the BBC that the legal power that had been relied on to exercise that authority was so broad and the information surrounding it so slight that nobody knew that it was happening.

I make these points to say that the Government, in my mind, should make operational cases from first principles for every single one of these powers. Simply because they have already been in use and simply because the agencies have interpreted law in a manner that they feel has made them lawful does not make them lawful. It is right that Parliament should receive a full operational case for each and every one of these powers. It is a matter of assessing not whether they are merely helpful or offer some form of value, but whether, given the scope of everyone's lives that they touch—after all, that is what bulk powers do—they can be vetted and scrutinised to make sure that they are both necessary and proportionate.

The Chairman: Thank you all three very much indeed.

Q208 **Shabana Mahmood:** I want to ask you about future-proofing the Bill. When the police, Home Office and others gave evidence to us, they were pretty robust in their view that these powers were sufficiently future-proofed against behavioural and technological change, as the powers were broad and wide-ranging. Other experts, in evidence, scoffed at the very idea of future-proofing, because of the pace of change in technology and how that impacts on behaviour in the online and digital space. What are your views on whether future-proofing is possible and, if so, whether that has been achieved in the draft Bill?

Professor Bill Buchanan: If there is one change that is happening in systems just now, it is a move towards the cloud. So like it or not, most of our emails are stored in the cloud, possibly in other jurisdictions. The main moves are with tunnelled web access. If someone uses a tunnelled connection, you cannot see the detail of the information that is passed. The minute someone uses https there is no way that you can see what page they accessed on the site; you can see the IP address but you cannot see what they clicked on. The whole world is moving towards https. Google is almost forcing companies to sign with a digital certificate or they will not be ranked highly. Many companies are moving towards adding a digital certificate. There is now a service online for free; you do not have to pay for a certificate any more. So increasingly companies will be signing their sites. Once they do that, communications are likely to be https.

There may come a time when many service providers will accept only secure communication. It is likely that our old protocols—http, Telnet, SMTP—will be switched off and replaced by the s version, the secure version. More and more people are using VPN connections. If you are a businessperson you will use a VPN connection if you are on the

road. VPNs cannot really be cracked at all. Along with that, more people are using proxy systems where the accesses are not coming from their own computer but from another computer. Increasingly we are using public wi-fi to access the internet. It is extremely difficult to trace someone who connects to, say, Starbucks wi-fi. Very basic registration happens, usually around email addresses, and many users would not feel that they need to put full details behind that. The increasing usage of Tor is a particular problem. With Tor, you usually will not see anything at all about the IP address of the destination because each link on the chain is encrypted with a special key so there is no way you can see anything from a Tor connection.

Shabana Mahmood: So tunnelled access—such as VPNs, which many MPs use to log in when they are not on the Estate, for example, and public wi-fi—is becoming the default and therefore not easy to crack.

Professor Bill Buchanan: We have created an internet that is based on legacy protocols. They were created a time when someone had to type in the commands manually. We now have browsers, graphical interfaces and so on. These protocols can be easily breached. They can be sniffed. Anyone who listens to the traffic can crack them. So increasingly businesses and individuals are protecting themselves through the usage of tunnels. Certainly if you are a business you must ensure that your communications are encrypted over public access. If you stay in a hotel room, if you are using the public wi-fi, how do you actually know that the SSID you connect to really is the wi-fi of the hotel? It could be some intruder next door. It happened in the Far East: a whole lot of hackers in a hotel room targeted businesspeople and were continually sending vulnerabilities to them. More and more we are encrypting traffic and setting up tunnels, and it is very difficult for the UK to drive these things because they are typically driven by the cloud providers such as Microsoft, Apple and Facebook.

Shabana Mahmood: On the cloud, people with smartphones go up to the Apple cloud automatically and you get a certain amount of space. Is there any difference in security between the free cloud services and the paid-for ones such as Dropbox, as well as in how much space you get?

Professor Bill Buchanan: Obviously you pay for the security that you get. Brand reputation is very important in this space. Apple, Facebook, Microsoft and Google have their brands to protect. If there was a large-scale data breach for any of those companies, it would decimate them. Banks and the finance industry have invested a great deal in the UK in protecting data and have gone through the CBEST penetration testing. Other companies, such as retail companies and internet service providers, have not gone through the same type of testing.

Erka Koivunen: The question was about future-proofing the legislation. I was puzzled by the introduction of the term "communications service providers"—CSPs. I was not familiar with that. Internet service providers—ISPs—and the telecommunications operators; that is the normal, old-fashioned way of referring to those carrier and access network providers. I was equally puzzled to find that in the actual text of the legislation, CSPs are not mentioned. There are references to what telecommunications operators would need to do and what information would be requested from them. To me, this sounds a pretty old-

fashioned way of approaching the problem of acquiring information about content or about whether an event took place in the first place. In that sense, I do not consider the Bill to be future-proof. Because there are so many references to bulk information gathering, it seems as though there is not even a proper attempt to go to non-traditional telecommunications providers to acquire the material that would be needed. Instead, the information and the traffic would be collected from the wire in bulk and then content or metadata collected with brute force, if you will. Of course, the equipment interference provisions in the Bill acknowledge that whenever you are unable to decrypt the material that you get online from the wire, you will need to go to the end point of the communication, where the material will be stored—hopefully in clear text.

I should point out that our company is actually one of the providers of those VPN type of tunnelling services. We provide a service where you can analyse yourself and encrypt your communication. You are able to move yourself virtually around the world so as to hide the origin of your traffic. Currently, we get only a handful of "targeted" law enforcement requests for the activities of our end users. I guess I am at liberty to tell you that none of them this year came from the UK. In this sense, I am a bit puzzled as to why there is such a pronounced need to get bulk information when even the old-fashioned, more targeted means to acquire information from communications providers are not being used.

Eric King: As upsetting as I am sure it will be if every few years we have to go through a Bill of this length and size, it may be what is required. This is an area that is inherently unsuitable for future-proofing because every year technology simply provides us with possibilities that our laws do not cover squarely or clearly. Where there is a grey area, our agencies have interpreted the law to give themselves the most expansive authority time and time again. Michael Hayden, the former director of the National Security Agency in the US, summarised this by saying, "Give me the box you will allow me to operate in. I'm going to play to the very edges of that box". I am not sure I can criticise him for that. I think that the permission our agencies have is very important and it is right that they use every authority and every capability at their disposal. Nevertheless, it is important that they exercise those powers only when they have been clearly authorised to do so by Parliament.

There have been a number of circumstances over the past few years where in this country we have found that that has not been straightforwardly followed. To my surprise, in the course of litigation involving GCHQ, Charles Farr provided a statement to the court which provided an entirely novel interpretation of what constitutes an external communication. He told the court that if you and I were sending a message using our phones, that would be classed as internal, but as soon as we switched to Facebook, or any other online platform, you and I were no longer communicating. Instead, I was communicating with Facebook, and so were you, and as a result they were external communications. As a result of that, fewer protections were offered to both you and me. It seems to me that that is not right.

We had a similar experience with intelligence sharing. I will not repeat what I know you heard from Amnesty earlier on that point. More recently, I was concerned to learn that, in particular, GCHQ and our security services have taken a very expansive approach on their authorisation of what constitutes a targeted warrant. It seems that thematic warrantry has now become slightly more default than any of us were aware. I was in court a few weeks

ago and heard the Treasury devil argue that the use of a general warrant—that is, that you could target on the basis of a class of persons—would be entirely permissible under the Government's current interpretation of the Intelligence Services Act, which they claim provides them with the ability to hack domestically inside the United Kingdom. These are all issues that the intelligence agencies have thought about. They have determined in secret the scope of their authority, and they are being challenged in these circumstances only because of a whistleblower who brought them to public attention. They have been brought before the courts and they are being tested. It seems to me that we will need regularly to update this law if we do not want to encourage whistleblowers to continue their practices year on year.

Q209 Lord Strasburger: Professor Buchanan, you mentioned the risk if you are in hotel of not knowing whether you are communicating with the hotel's wi-fi or something else. I have been in that position and have had my phone intercepted. It was a demonstration that was organised by F-Secure, so I declare that interest.

On the subject of future-proofing, we have heard many times during these proceedings about the very broad way that various parts of this Bill and other Bills in the past have been drafted. The explanation that we hear from the Home Office is that this is to allow future-proofing so that it can massage the definitions as time goes by. Mr King mentioned this, but neither of the others did. Is the answer to have a new Bill every Parliament, which would be every five years?

Professor Bill Buchanan: I go back to my main point that I can see cryptography and the use of tunnels increasing. There is no Bill in the world that can crack an encryption key that has been created for every connection that you make. You can legislate for it, but technically, it is not possible. The state of the art is 72 bytes. If you tunnelled on every single computer in the whole world, in a month or so, you could just crack a 72-byte key. The keys we are now using are 128 bytes or 256 bytes. It is double, double, double, double until we get to 128. It would take you a lifetime to crack 128-byte keys with current technology.

The Chairman: Is that a yes or a no, Professor Buchanan? Do you think they should be?

Professor Bill Buchanan: I can only say from a technical point of view, from a cryptography point of view, that the Bill would have to provide that cloud service providers would have to hand over the private key, have a key in escrow or have some backdoor, some proxy, on a machine. That is the only way that you would crack the cryptography problem.

Lord Strasburger: I was not talking specifically about cryptography; I was talking about all the provisions in the Bill in order to keep the provisions of the Bill current. Do we need to come back to it roughly once every five years and have a new Bill?

Professor Bill Buchanan: Certainly the way that computing is moving the pace is unstoppable.

The Chairman: Mr King, Mr Koivunen, can you say briefly, as we are beginning to run out of time, whether you agree with Lord Strasburger that we as a legislature should be renewing these provisions every so often because of the changes in technology?

Erka Koivunen: Definitely. I am a big proponent of transparency and the democratic process. Intrusive methods, such as these, should be reviewed.

Eric King: Yes, although I do not think that that should lessen the scrutiny that is put in place for this Bill.

The Chairman: On the principle of renewal, all three of you—or two of you at least are not quite sure—would be in favour.

Q210 Dr Andrew Murrison: Do these keys exist, or would they have to be created?

Professor Bill Buchanan: Do you mean the keys of the tunnels that are created or the keys that are held by the cloud providers?

Dr Andrew Murrison: The keys that are held by cloud providers.

Professor Bill Buchanan: A survey was done recently of some of the largest companies in the world. They had an average of more than 17,000 encryption keys—key pairs, as we would call them. A public key is known by everyone, the private key is what you keep secret. If someone finds the private key, they can crack the communications. The majority of companies do not know how many keys they have. Keys are being created at any given time, but companies such as Google will have a master private key which is used for its communications. That key is updated regularly. It might be six months or one year or so. That key will stay active for that amount of time. There is a revocation service on the internet that does not quite work. If the keys have been stolen by someone, what is meant to happen is that all the browsers will no longer accept that key. Unfortunately, Google Chrome does not accept revocation services by default. The keys are actually created by the cloud providers, but every session we create with our cloud services has a new key every time.

Dr Andrew Murrison: I suppose that is our safety net, is it not? We are worried about government having this information, or having access to information through keys. However, the gist of what I am asking is, are we at the moment at the mercy of providers such as Google?

Professor Bill Buchanan: Yes.

Dr Andrew Murrison: Yes, thank you. That is no comfort, is it? There are a number of these, and we presumably have no control over their internal security mechanisms, except as far as their reputation is concerned.

Professor Bill Buchanan: Only 5 per cent of SMEs have any auditing facility with their cloud provider. Only about half of large companies have some form of auditing that they can actually have on cloud services.

Dr Andrew Murrison: Thank you. Can I ask you about definitions in the draft legislation that we have seen? We have a range of descriptions, particularly in relation to communications data, such as entity and events. You might be forgiven for thinking that Sir Humphrey had drafted some of these, because to a lay person they are certainly approaching meaningless. I would be interested in your thoughts on the definitions and whether you think that they are

simply creating the aforementioned box and are drafted in such elastic terms as to be maximally obliging to those in the agencies who want to pursue this data. We have mentioned, for example, the thematic warrant. It is not entirely clear to me what a thematic warrant is, and several witnesses have already said that they are concerned about the fluidity of some of the definitions used in the Bill. I would be interested in your views.

Eric King: As a broad, concerning criticism, the definitions here leave a lot of room for manoeuvre. On issues such as thematic warrantry, it is less the term "thematic warrantry" itself but the scope of the language surrounding that that worries me. The ability in particular to add and remove individuals seems very broad. The more technical terms "events" and "entities", while new to all of us, are not new to the Home Office; they are the terms that GCHQ itself has used for the past decade. GCHQ is very familiar with them and has been exploiting them to the full for a very long time. Events and entities in particular are the issues that are of most interest to our security agencies; these are the capabilities that provide them with the most amount of information. The ISC helpfully said earlier this year that, "the primary value to GCHQ … was not in the actual content of communications, but in the information associated with those communications". I can give you a longer list, but it is very important that these definitions are tightened. A number fall in the gap. As an example, if a telephone call is intercepted and GCHQ identifies the gender of the speaker, is that an event, an entity, content? It is unclear to me.

Q211 Suella Fernandes: Clause 12, Part 2, relates to interception and refers to related communications data. I should say that new Clause 12 replaces the existing Part 1, Chapter 1 of RIPA, so it is a power that already exists. With reference to the point about related communications data, in brief it relates to communications that have been intercepted in relation to the postal service and telecommunications systems, and to assisting with the identification of a telecommunications system, an event or a location. What is your view on the clarity in that clause of the term "related communications data"?

Professor Bill Buchanan: A key aspect of this is that the IP address can never really be trusted, and any digital information that you gain typically from a home environment or electronically, again, cannot be trusted. If someone is in a home environment, they are typically on a private network and they are mapped to a single IP address, so it is very difficult to pick off the person who is actually communicating. So the ability to cross-correlate it with other information, such as location information and calls, is certainly a step forward in providing credible evidence for corroboration. This evidence on its own really should not be seen as an opportunity to look at a single source and to be able to determine the evidence from that. A great worry from our point of view is that within a private network it is very difficult to pick off individuals, so anything that can be added to that certainly helps.

Erka Koivunen: I am an engineer by background. To me, there is only the content, the payload, that we are protecting and then the metadata that describes who was communicating and where the communication was going to. There is other related information such as what type of encryption and network protocol was being used. I read with great interest about the events data, entity data and related communications data which this Bill would recognise, but to me it sounds as though you would need to tap into the network, take all the data and then start peeling the communications so that you could

drop the actual payload. Afterwards, when you start dissecting the communications data for law enforcement and intelligence purposes, these terms become relevant, but when the data is acquired it does not matter how.

Eric King: In the interests of time, I will say no more than what I said previously in answer to Andrew Murrison, other than to agree with the best analysis that I have read on this point. It is by Graham Smith, who I believe you have had before you already. I know that he submitted something to the Science and Technology Committee on exactly this question. It was a masterful dissection of a complicated set of questions. I will not attempt to explain it here for fear of embarrassing myself or doing his argument an injustice, but it is one that should be rated very highly.

Q212 Lord Butler of Brockwell: I think you have partially answered this question already, but I will just ask whether you have anything to add. How clear is the definition of internet connection records in the Bill, and is it practicable to get a clear definition that will meet the purposes of resolving the IP identity?

Eric King: The first thing that needs to be remembered about internet connection records is that it is not a term that exists naturally, unlike phone billing records. It is an invented set of ideas. As a result, the first thing we should do before putting new authorities in place is wait to see the outcome of the IP resolution efforts that were made earlier this year with the Anti-terrorism, Crime and Security Act. It is still only months since that Act was passed. Its goal was to provide for IP resolution, which is the same stated goal in this Bill. It is unclear to me why we have not waited to see the fruits of that, to see where the gaps may or may not be, and to learn lessons where we can. The closest I have seen to any state attempting this elsewhere is in Denmark, which had a similar scheme over recent years but stopped it—two years ago, I believe—after it was found to be ineffective. With that, my caution would be to say that we should learn that lesson and wait for any lessons that we can learn from the IP resolution measure that was passed earlier this year.

Lord Butler of Brockwell: Going back to our earlier discussion, is not the answer that this is just a power, so the Home Office could wait for some time before it exercised it? Would you have any objection to this power being in the Bill?

Eric King: I think I would. I am not sure that the blanket retention of communications is a proportionate activity per se. In the Digital Rights Ireland case last year, the CJEU struck down a similar authority for telephone records. My position at the moment is that we should not be legislating at all in this area until cases that are going up to the CJEU are resolved, for fear of us all wasting quite a lot of our time and having to re-amend and re-adapt the law, particularly given that we could be waiting to see how the Anti-terrorism, Crime and Security Act is implemented. I think we should hold back in this area and not include it in the Bill at all.

Lord Butler of Brockwell: Do your colleagues have anything to add on ICRs?

Erka Koivunen: I would like to continue with a Danish example. I have been told by my old Danish colleagues at DK-CERT that there was an attempt to mandate that all public wi-fi providers should be required to keep session logs of where their users were communicating to. This would include not only telecommunications operators but cafés, conference halls

and airports. I used to work for a telecommunications provider and we used to call these cafés hobbyists. These hobbyists would be required to gather sensitive information about who their users were communicating with and they would need to retain that information and have it available whenever law enforcement requested it. To a cybersecurity professional, that spells disaster. It is a disaster waiting to happen. Each and every store of this kind of information would be a target for computer intrusions by criminals and foreign intelligence services. One also has to remember that it would be pretty expensive for the service providers to start collecting that. In Denmark, in the end, that is why the so-called hobbyist providers were exempted from that legislation, and eventually that whole law was scrapped.

Professor Bill Buchanan: I go back to my point that proxy systems hide the IP address of the sender. Tunnelling systems hide the content. Tor systems hide the content and the IP addresses of the sender and the destination. VPNs hide the content and the source address. Many people are moving to cloud-based systems: you can run virtual desktops within the cloud. The concept of running things on hardware is going. We are moving towards almost a mainframe-type system. We have a terminal that we connect to the cloud and the cloud exists somewhere else on the internet. Anyone who is even a little bit tech-savvy is able to pick one of those systems and hide their logs. Providers need to think through all the options and collect other information which can then be used to corroborate with the pinpoint of information that you might get from an internet service provider.

Lord Butler of Brockwell: So you would conclude that, in its present form, this is not value for money?

Professor Bill Buchanan: In its present form, from a technical point of view, it can be very difficult to find the information that is actually required from purely internet-based records. There is a whole lot of other information that we leave behind. If we have a mobile phone we can be tracked every time we make a call, and so on. There is a whole lot of other information that could be used alongside the internet record. This is not the catch-all that it could be. Ten years ago it was: you could look at anyone's record. The one company that has the whole record of every little thing we have done on the internet is Google. It has all our information. That is because it is the end point. It is the place that you go to and it will see all the information. Unfortunately, that jurisdiction is not inside the borders of this country.

Q213 **The Chairman:** Clauses 51 to 53 of this very long Bill talk about a request filter. What are your views on that?

Eric King: If I may, I would like to get back to the Committee on that, once I have some questions clarified by the Home Office about the exact scope of what it intends. My starting point is that it permits the same sort of data-mining at a scale that so far only our intelligence and security agencies have been undertaking, and provides that to the police, but in the name of a safeguard. Regrettably, a more detailed analysis requires more information but I will be very happy to provide the Committee with that once it is available.

The Chairman: Would you like to comment on that?

Professor Bill Buchanan: It is certainly a good way forward. Some sort of definition of the search terms that would be used would protect us from a large-scale data breach. The last thing we need is for all the information from an ISP to be leaked because a log was allowed to be taken of its site. The logs should be kept in a trusted environment and the access to them should be locked down to IP addresses and to biometrics if possible. Because they are probably among the most sensitive logs that we have, if we make sure that the requests made actually match what has been collected, we can make sure that a summary record is given to law enforcement, not the full record. Systems are easily breached. You can take data quite easily from them. It is very difficult to protect them. An abstraction around a request filter is a good way forward.

Q214 Lord Strasburger: Is it reasonable and practicable to require communications service providers to remove the electronic protections from their data when providing it to law enforcement agencies and the security and intelligence services?

Eric King: This issue has taken on increased importance due to how it seems that the Home Office wishes to apply it in future. If it intends to use it to force companies such as Apple to remove encryption or to re-architect their systems to provide a backdoor, that would be wholly inappropriate. It would provide a lesser degree of security for us all. The Home Office needs to answer many more questions as to how it intends to use this authority. If the companies' public statements on this issue are to be believed, we should all be concerned.

Erka Koivunen: From a technical point of view, if the telecommunications operator which has been served this kind of information request is able to remove those protections, which are typically provided through encryption, of course it would make sense for these protections to be removed to enable the law enforcement and intelligence agencies to make any use of the data that they receive. However, echoing what Mr King said, there are many stakeholders in these communications service providers. Some of these providers have designed their systems specifically to employ end-to-end encryption, where the service provider is not in a position to open up the encryption. The encryption goes through the service provider's systems so that even the provider is not able to see through it. The way I am reading the Bill, it would actually ban the use of strong cryptography and strong encryption and would essentially weaken our ability to use secure online services.

Going back to the question of future-proofing, as a company that provides systems where we potentially are not able to decrypt the traffic that we pass—

Lord Strasburger: Sorry, did you say "are" or "are not"?

Erka Koivunen: We provide services that we would not be able to decrypt ourselves. We are not sure whether the Bill would concern us—whether we would be compelled to redesign our systems. I imagine that Apple will be reading the Bill with a similar sentiment. I think that it would refuse to redesign its systems in a fashion that would open up and weaken the encryption. So the Bill has some problems in the way it has been written.

Professor Bill Buchanan: Cryptography and the methods that we use in cryptography are almost perfect. Unfortunately, it is the humans who implement it who are flawed. The humans who implement security, too, are often fairly flawed in their approaches. If you ask

most people whether they trust that their ISP's or CSP's security is robust enough to handle secure information such as this, I think the majority would say no, especially after the TalkTalk hack. I have many examples of where they use weak passwords and so on. If we have now got to the point where our banks can be trusted with data because of the CBEST standards and can be put to the onerous task of protecting records such as this to provide lots of different levels of access, then the ISPs and CSPs have to up their game many times over. They have typically grown from telecoms providers and have been merged from lots of little companies to provide big, heterogeneous types of organisations that are difficult to control.

The only way is with multifactor authentication. The idea that you can open up some data or a log with a single key or a single password has gone. The controls and the proving of identify is key to providing access to the data. The data should never appear offsite at all. The only way you should be able to access the data is by remote access and only through a portal. If we were to risk the opportunity of downloading a whole aggregated log on to a machine with a single encryption key then we really are opening a can of worms. CSPs and ISPs need to be thinking about access. Certainly there should be some biometrics in there—fingerprint recognition at least, along with geolocation, so that only certain locations would be allowed access to it. A mobile phone, through out of band identity methods, is also a good way. You really must wonder, "If my password is changed by my mother's maiden name on my ISP, anyone can find out my mother's maiden name fairly simply from an internet search". If that is the level that ISPs and CSPs are now at, they need to recruit a whole lot of security engineers, architects, cloud engineers and so on. They need proper investment because this will be a massive task. The banks are soaking up all of our graduates to work in these types of environments. The next wave is that if the UK cannot produce enough cybersecurity specialists, where will we get all these new specialists? The country needs to think ahead and, I hope, invest with the ISPs or CSPs to make sure that they protect our data.

Lord Strasburger: What are the risks and benefits of allowing law enforcement and the agencies to undertake equipment interference? I mean both types of equipment interference, targeted and bulk.

Eric King: On the law enforcement side, the most powerful argument I have heard for preventing law enforcement having access to equipment interference was from the Suzy Lamplugh Trust earlier: the powers they are currently provided with are not being used to their fullest. Given the incredible intrusiveness that equipment interference could provide law enforcement, we should treat it with extraordinary scepticism. One of the issues at the front of my mind and which I have not had an answer from police or the Home Office on is how we will get around the issue that, by deploying equipment interference—what the agencies sometimes call "computer network exploitation"—we will not damage evidence that the police would later wish to seize and rely on in court. It seems that it would be incredibly counterproductive to be providing an authority in this manner that, in some circumstances, could result in criminals getting off the hook. Until I hear a compelling answer from the Home Office on that point I am not sure that we should move forward with that aspect.

In the intelligence domain it is far more severe. I struggle to understand exactly what the Government have in mind by bulk equipment interference. Every single scenario that I can conjure up seems to be within the scope of what are the not very targeted but nevertheless called targeted equipment interference powers that are there. That is because it provides them with thematic warrantry or even hacking by location. That by itself is very broad. We need to understand that, by undertaking interference, our agencies threaten British cybersecurity. They regularly hack companies in Europe and elsewhere that are not a national security threat in and of themselves. The employees of those companies are not suspected of any serious crime or criminal wrongdoing, but these companies are being attacked to allow GCHQ and other agencies to undertake further attacks. In recent years, we found out that GCHQ hacked Belgium's largest telecoms provider, Belgacom. It has also hacked Deutsche Telekom, Seagle, Stella—the list goes on and on. In doing so, they are painting targets on British companies' backs in exactly the same way and legitimising these kinds of attacks. By attacking using vulnerabilities in networks and systems that they have acquired themselves but are refusing to tell the world about so that those companies can protect themselves, they reduce the security that we collectively experience. The stockpiling of these vulnerabilities in zero-days is not considered in the Bill. Policies need to be very clearly set out about it before any consideration is made of the powers. As it stands, our recommendation to the Committee is that bulk equipment interference should be absolutely prohibited. There seems to be no good reason why such a thing could be undertaken. Should equipment interference be permitted at all, I point the Committee to the recommendations made by Privacy International and the Open Rights Group as a result of the draft equipment code of practice introduced earlier this year in response to recommendations.

Lord Butler of Brockwell: May I ask one short supplementary on that? You say that we are putting British companies at risk by pinning a target on their backs. Foreign interceptors are not going to intercept British companies just by way of revenge, are they? They will do it anyway if they want to.

Eric King: I would hope not. Nevertheless, by using vulnerabilities and imagining that we are the only state that has discovered them we allow British companies to continue to be exposed to those threats. Instead, when British agencies find a vulnerability in networks, their presumptive position should be to disclose that to the appropriate vendor so that all companies can benefit from that security. Instead, by keeping them and using that as part of attacks, we first raise a flag, so that when those attacks are eventually discovered others will use that same attack here in the United Kingdom. Secondly, we are preventing them from being able to defend against attacks that we could be assisting them in preventing in the first instance.

The Chairman: We are getting very close on time now.

Erka Koivunen: The term "equipment interference" is pretty elegant. When I was learning information security at school we used "exploitation", "vulnerabilities" and "attacks" to describe the same things. There was no discussion of vulnerabilities or attempts to let the vendors of software products know about them. Equipment interference also refers to the deliberate introduction of those vulnerabilities and backdoors in products. In recent days, we learnt that Juniper, a big provider of core networking components that the internet is

being built on, found backdoors and means to weaken encryption in its systems. This backdoor was in its code for at least two years. This was probably of use to some intelligence organisations' operations around the world. However, the UK networks, the Finnish telecommunication providers' core networks and the corporations' networks are being built by the exact same systems. They have been vulnerable to this type of exploitation for two years already and are not rushing to patch their systems. Cisco Systems had a similar case a couple of years ago that was not publicly discussed. There are many systems where it has been suspected that vendors have been compelled to introduce backdoors of this nature to deliberately weaken cybersecurity protections in favour of some intelligence organisations. I see this as a threat to civilian society's ability to conduct business online, and to e-government processes. When we cannot trust our information-processing infrastructure, we tend to avoid using it to conduct business.

The Chairman: Very briefly, Professor.

Professor Bill Buchanan: My view is that virtually everything is possible and it should be based on a risk-based approach. If something is high-risk these things should actually happen and we should be looking at exploiting vulnerabilities. As long as there is a reason for doing it and it is documented and audited, really anything is possible from a technical point of view.

The Chairman: Thank you very much indeed. Mr Warman, you have a final question before we move on to the next session?

Q215 **Matt Warman:** I should declare that my wife is a student at Queen Mary, but not one of yours so do not worry. If we look round the world, how does this compare to international legislation that is coming forward or is currently in force?

Professor Bill Buchanan: In France just now the access to public wi-fi is being looked at. In Kazakhstan, of all places, they are looking to implement a digital certificate where you cannot connect to a secure channel unless you use the Kazakhstan certificate. Unfortunately, the problem with that is that none of the cloud providers trust that certificate, which means that it could decimate their business and the social aspects. It has been done with the aim of improving privacy but there may also be a political agenda. It has also been shown that general certificates can be hacked. It happened when Iranian hackers got access to the DigiNotar certificate, which was a Dutch certificate, and managed to hack 300,000 users on Google and listen to their communications. Most countries are now looking at the inability to view logs. Few countries have been able to get the balance right.

Erka Koivunen: As a matter of fact, I am participating in the reform of the Finnish intelligence legislation and there are discussions about targeted equipment interference, using the terminology in this Bill. There is a pretty wide consensus that attacking foreign military installations will be something that we will see parliamentary consensus on next year, when it goes to parliament in Finland. The intelligence services in Finland have already publicly stated that they are refraining from demanding backdoors and the weakening of encryption while they seek a new mandate.

Eric King: There are lots of comparisons we could look to but we should focus on the United States as a country that we share a very similar capability with; under the Five Eyes Alliance, we also have much the same approach to issues. Over the past two years in the United States, reforms have been made to curtail NSA capability. There is one power in particular that I bring the Committee's attention to, and that is to do with bulk communications data acquisition. This is what was avowed by the Home Secretary to the Commons when introducing the Bill. While we have very little information about how this is used in the UK, in the United States this was on the front page of most newspapers. Very helpfully, two independent bodies that had access to classified material were able to look at the programme and consider it in detail. The President's Review Group on Intelligence and Communications concluded that the use of this was not essential to preventing attacks. Similarly, the Privacy and Civil Liberties Oversight Board concluded that, "we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot". This is a power that there have been two detailed reviews on in the United States and that they have decided to end. Indeed, it was just a few weeks ago that that programme was brought to a close but here the Bill is attempting to place it on a statutory footing for the very first time.

Matt Warman: That is not a technical point—if our agencies were to say that they thought it was necessary for national security, there is not a technical argument for making the observation that for political purposes or whatever they have made a different decision in a different country?

Eric King: In the country in which an operational case was made, that could be scrutinised by a series of very senior experts—who in many circumstances were very close to the intelligence community—who had access to classified material, who looked in detail at the operational case and found it lacking. My presumption is that the Committee should take the same approach until such a time in which the security services provide a public rebuttal and can show that the operational case is somehow different from the one that was so carefully scrutinised by so many people in the United States.

The Chairman: Thank you very much, all three of you, for a very interesting session, particularly Erka for coming a long way at relatively short notice. We wish you a very happy Christmas.

Sir Stanley Burnton, Interception of Communications Commissioner (QQ 47-60)

Evidence heard in public Questions 47-60

Oral Evidence

Taken before the Joint Committee

on Wednesday 2 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Stuart C McDonald MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Bishop of Chester, Lord Hart of Chilton, Lord Henley, Lord Strasburger.

Witness: **Sir Stanley Burnton**, Interception of Communications Commissioner, gave evidence.

Q47 The Chairman: Lord Judge, Sir Stanley and your staff, thank you very much indeed for coming along to us this afternoon. As you know, this is a very important Bill. The Prime Minister described it as the most important of this Session. Much of the Bill refers to the change in oversight provision, so we are very grateful for your coming along. I wonder whether you want to say anything yourselves before we start asking some questions.

Lord Judge: I would like to say something, particularly in view of the discussion that has been going on with Sir Mark. I cannot think that anyone would have designed the present three-bodied system. It would never have happened; it should not have done. We work piecemeal on the legislation; we produce piecemeal results; and we have produced three bodies, all of which have responsibilities in the broad sense that we are talking about and all of which work in different ways.

Let me give you some "for instances". Sir Mark has just given evidence to you. He is the commissioner. He has no inspectors. Sir Stanley will tell you that he is the commissioner and, with his team, he has 10 inspectors. I will tell you that I have taken over the surveillance commission. I have seven inspectors, who are former police officers of no less than superintendent level, a Chief Surveillance Inspector, six commissioners, three assistant surveillance commissioners and, good heavens, there is even me. We all operate differently. The focus so far has been on Sir Mark, and I know that IOCCO, as it is called, has had quite a lot of input, but can I just explain to you how this leads to confusion and can be improved?

The Chairman: Please do.

Lord Judge: We have had to take on oversight and prior approval of undercover police authorisations. We all know about the relatively recent disasters caused by officers going wrong in undercover operations. There is an application to us and, mark this: we have to authorise. Neither of the other two Commissions authorises. Every single piece of intrusive surveillance, certain types of property interference and long term undercover operatives

for which we are responsible is authorised in advance by a commissioner, who is a former judge.

The case is made out to us that there should be an undercover police officer in this particular, rather serious drugs case. The authorisation is made. In goes this brave young man or woman—and most of them are very brave young men and women—and they discover that there is quite a lot going on and it would be a good idea to have some intrusive surveillance, say into a car that is being used to transport the proceeds of drugs. He has to go back to his authorising officer. The authorising officer comes to us, and there is another application for intrusive surveillance to take place. That takes place, and that reveals something else: these drugs are actually to do with a potential terrorist ring.

That does not come to us; that goes to Sir Mark, but there is no pre-authorisation by him. Somebody says, "We had better have some communications input". That goes to Sir Stanley. There is no pre-authorisation by him. Now, I am sorry to say this, but telling the story the way I have is entirely accurate. If you thought about it, you would say, "Is this really the way we are doing business?".

Speaking only for my own team, every authorisation is made before any of the aforementioned intrusion takes place. The papers come to us, and I have a complaint about the quality of our equipment, but that is another question. A judge commissioner looks at them. He decides whether necessity is established and whether it is proportionate, which involves looking at the nature of the offence. You would not authorise intrusive surveillance for somebody who was stealing a tin of salmon from a supermarket. You are looking at sentences starting in the three to four-year range and upwards. He checks for proportionality: is this a reasonable way to go about sorting this problem out? He authorises or does not, or says, "I want more information". Then the process goes through.

At the other end of the process, every year my inspectors go in and conduct an inspection of every single police force in the country, Her Majesty's Revenue & Customs and so on—all the law enforcement bodies. They conduct random analyses inspections of all the things for which the body is responsible, such as encryption. There are all sorts of different things that come under the remit of covert surveillance. They then write a report. The report is written to me. It goes to the chief constable. I write my own report to the chief constable. Sometimes I say, "This is being very well handled. Your authorising officers are well trained. The paperwork is very good. The explanations are excellent", and so on and so forth. I have just written a very rude letter saying, "This is not good enough. You are not complying. There are too many breaches. There is too much inefficiency in this part or that part", or whatever it is.

I write that to the Chief Constable, and then I go and see him, or one of my commissioners does. I go to all the big Forces. We discuss the report for the year. Most of the time—and this I hope does not surprise you—the chief constables are as anxious as we are that the job should be done properly. Apart from the reputational matter, they are men, and women now, who want the job done lawfully. They are also aware of the dangers of evidence being excluded at the trial process or an abuse of process argument leading to the whole prosecution being discontinued. I go there; we discuss it. If I am unhappy, I will go again. I have not had to, but I have only been in this job for a relatively short time.

I am not recommending it to you, but our system is very different from the one you have been discussing with Sir Mark, and from Sir Stanley's. The idea that we should have a surveillance system in which there are three different bodies is itself absurd, and then three different bodies operating differently strikes me as daft. That is my opening statement.

The Chairman: Very interesting it was, too. Sir Stanley, do you want to make any comments?

Sir Stanley Burnton: As you know, I am the new boy on the block. I have the good fortune to have staff who have received a glowing report from David Anderson, as you will have seen. They have a range of competencies, including computer abilities. There were questions asked of Sir Mark about training. I have some computer knowledge; I was judge in charge of IT, but I could not go into a public authority and interrogate their computer system. We have inspectors who can and do just that.

We carry out an audit function. I believe that you cannot carry out an audit function properly unless you have some understanding of the business you are auditing. That does not mean to say you could do it yourself. I could not go into a computer and interrogate it to see how many search or interception warrants had been issued, and view the grounds and so on. But I like to think I have a sufficient understanding of what staff can do, and do, to carry out the functions of my office.

Like Sir Mark, as far as I am aware, there was no special security clearance carried out when I was appointed. On the other hand, when I was a judge, I used to do Special Immigration Appeals Commission, or SIAC, cases, which concerned terrorism and people who were alleged to be terrorists, so I have some acquaintance with that part of the job. Of course, I did criminal work, so I have some acquaintance with that area as well.

Q48 **Lord Butler of Brockwell:** May we take it from Lord Judge's and Sir Stanley's opening statements that you think it is a good idea that this Bill in future sets up a single Investigatory Powers Commissioner?

Lord Judge: I have no doubt about that. We also have to make all the three current bits of the system work in the same way. I personally think, although I have no experience of IOCCO or Sir Mark's work, that the authorisation process is one of the strengths of what we do. You have to have an authorising officer who persuades you that this is appropriate—i.e. necessary and proportionate.

Lord Butler of Brockwell: If I may then clarify my understanding of this, in your area, Lord Judge, there is pre-event judicial authorisation.

Lord Judge: Of every item of intrusion that comes within our jurisdiction for prior approval by a Surveillance Commissioner.

Lord Butler of Brockwell: In Sir Stanley's area, this Bill will set up, except in the most urgent cases, pre-event judicial authorisation. Is that correct?

Jo Cavan: It will in relation to interception warrants, but it will not in relation to acquisition and disclosure of communications data, which is the bulk of our remit. Around 500,000 requests for communications data are made on an annual basis, by a rather large number

of public authorities. The judicial authorisation and the double lock that the Bill introduces are only in relation to the interception warrants, of which there are around 2,700 a year.

Lord Butler of Brockwell: Thank you very much. Then, if I understood what Sir Mark said, in the case, however, of somebody placing a bug in premises, there will be no judicial pre-event authorisation. There will be a warrant, but there will not be a judicial pre-event authorisation.

Lord Judge: If it is an application under part 3 of The Police Act 1997, which we deal with a lot, there will have been a pre-judicial authorisation in advance (for activity in a private vehicle or premises). This is why the system desperately needs to be shaken up.

Lord Butler of Brockwell: What about in the case of the intelligence agencies? Did I misunderstand Sir Mark?

Lord Judge: No, you did not. The intelligence agencies work differently. If it is an ordinary police investigation, yes, every piece of intrusive surveillance is pre-authorised. In the case of intelligence, it works differently.

Lord Butler of Brockwell: In the case of an intelligence agency, at the moment and under the Bill as proposed, there is no pre-event judicial authorisation of the warrant.

Lord Judge: No.

Q49 Suella Fernandes: What do you think about the safeguards provided in the new system as compared to the current one? Do you consider that there are better safeguards under the proposed system?

Lord Judge: I think that pre-authorisation is something Parliament needs to look at across the board—but I would, wouldn't I, because I am convinced about our own little bit? If you do that, the papers come through to a commissioner, who knows what the law is, knows what he—or she, but we do not actually have any females—is looking for. If it is not good enough, if it is an urgent or relatively urgent thing, he speaks to the authorising officer, saying, "This is not good enough. Tell me more about this" or, "I am worried about the possibility that this suspect's wife is going to have her life intruded on". If satisfied—and usually you are, because they do not come unless they have a good case—then it is authorised. Then you inspect at the other end and you go through them.

I will add this, which I did not mention when I made my opening statement. From time to time, my inspectors will tell me that they are very worried about the commissioner having given an authorisation. They are not just examining the way the police are doing their work; they are a form of check that the commissioners are applying the law. Of course, it does not happen very often, but that is part of the process and I welcome it. If there is a case where I think the commissioner was wrong to make the authorisation, then I see him and say, "I think this was wrong" or whatever.

Provided that you, as the citizen, are satisfied that, before people can come intruding in your life, a decision has been made by somebody independent of those who are going to do the intrusion, and there is a system for inspecting afterwards, at random, what the various bodies have been doing, that is a pretty good form of safeguard. In my experience—

again limited—I do not see cases where people or authorities are applying unless they have good grounds for doing so, because they know they will be refused.

Q50 **Lord Strasburger:** My questions are for Ms Cavan. I would like to start by congratulating you on the transparency of your reports and your engagement with the public through Twitter. I wonder if Mr McDonald's concerns about systemic difficulties and unwarranted activities would be allayed by the new commissioner being able to initiate inquiries on his or her own initiative, and perhaps even unannounced inspections. That is my first question.

Jo Cavan: On that note, we recently published a wish-list of some of the ways we feel the oversight provisions need to be strengthened. In one respect, the ability and mandate of the new commission to launch inquiries or investigations, we feel, could be further strengthened. We also feel that access to technical systems could be more explicit in the clauses. At the moment, the drafting is outdated: it refers to providing the commissioner with information or documents, whereas these days we are generally not looking at paper. When our inspectors go in, they have full access to the technical systems; they run query-based searches and look for compliance issues at scale, which is really important when you are dealing with these bulk collections. We think the oversight provisions and the clauses concerning technical system access and the ability to launch inquiries and investigations could be strengthened further.

Lord Strasburger: Lord Chair, would it be appropriate to invite Ms Cavan to put her views on how that might be strengthened to us in writing?

The Chairman: I am sure that would be fine.

Lord Strasburger: My second question is: how do you think we should strengthen oversight of international co-operation between Five Eyes intelligence agencies?

Jo Cavan: There are some additional safeguards in the IP Bill for the sharing of intelligence with overseas agencies. These matters have been significantly debated during some of the recent Investigatory Powers Tribunal cases. As a result of further disclosures made in those cases by the Government, the safeguards have been published and they are now in an amended code of practice. Certainly, that is an area we are looking at during our inspections and audits.

Sir Stanley Burnton: The fact we can interrogate the computer records of the authority whose activities we are auditing reduces the need for unannounced visits, because we have access to the raw data.

Q51 **Victoria Atkins:** Following on from Lord Judge's very helpful analysis of the oversight and review process, there is one angle that I am not sure the Committee has heard about yet, which is what happens at trial. Where an investigation results in a suspect being charged and a prosecution being brought, could you help us, please, with the duties on the prosecuting lawyer and prosecuting counsel to ensure that any warrants that may have been used during the course of that investigation were conducted properly, and the professional obligations on them as a reviewing process, in addition to all the reviewing processes you have already described?

Lord Judge: When everything has worked as it should have, and there has been no breach and no subsequent concern, that simply goes through. There is no disclosure. But, where there has been any breach—and, as Sir Mark pointed out, there are self-reporting breaches as well as discovered breaches—it comes to me, and it is axiomatic that the first thing I do, having decided what should happen about the breach, is to say all the papers must now be retained and disclosed to the Crown Prosecution Service, in the event of a prosecution, for onward disclosure as seen fit. That is up to the prosecutor. That material, I am sure, would then go to counsel for the defence, who would then decide whether to make an application or not.

The other feature, which has been underlined by a recent decision in the Divisional Court called Chatwani, is that there is an obligation—it is obvious that there is, but the court has said so—on the person making the application to tell the whole truth. In other words, you set out the points you say are favourable to the application you are making and the authorisation you are seeking, but you also have to add the bits that do not fit. Chatwani was a case where what was going on was not properly disclosed and the Divisional Court said, "Quite obviously, you cannot work on the basis that the whole story is not told". Failure to tell the whole story would itself constitute a breach, which would then have this system fall into place: retain it, keep it, disclose it if there is a prosecution. Of course, often there is not a prosecution, which raises a different problem, but if there is that is how it is done.

Victoria Atkins: In addition to the many sets of eyes in your organisations, there is also, if a case comes to court, the extra review conducted by lawyers and counsel to ensure that processes have been applied properly.

Lord Judge: Yes.

Q52 **Baroness Browning:** You heard me ask Sir Mark about training. I wonder what training you feel might be necessary for the new judicial commissioners.

Lord Judge: Rather like Sir Mark, what you are doing is making a judgment. This is what, if you are a former judge, you have been doing for however many years you have been doing it. You have been making decisions like this day in, day out. The questions are very simple: is this necessary? Where is the evidence? Yes, on this evidence, it is necessary. Is this proportionate? I must bear this in mind and that in mind, and that in mind. On this evidence, that is proportionate. Hang on, there is a bit of this that might involve the suspect having had conversations with his, for the sake of argument, doctor. You have to be careful there. I mentioned earlier an intrusive surveillance into the family car that is being driven by the wife. Nobody suspects her of anything, so you cannot have that; it is not proportionate.

That is all you are doing. You are making a judicial judgment, which is what you have spent your whole career doing. I am not saying you are infallible, and I made the point a few minutes ago in relation to my commissioners: when they get it wrong, my inspectors will tell me. But you do not need special training for that. What happened to me is, in effect, I went and shadowed my predecessor. I went out on inspections to see what my inspectors did and how they went about it, and to see that they were doing the job the way I wanted

them to do it. I go out with my commissioners. We meet regularly and discuss the problems that are current. That is the training, and then you take over the job.

Baroness Browning: With the advance of technology and things moving on so quickly, particularly once this is in one collective body, could the choice of methodology in the application that comes before you be something you question—whether this route is going to be used or that route? Does that not require some technical knowledge on the part of the person making the decision?

Lord Judge: Not really, because, for necessity, that does not arise. You do not need to know whether the nature of the intrusion is a probe that is one inch long or six inches long; you need to know whether there is going to be a probe. Of course, I have overlooked this. I spent time, two days ago, sitting in the National Crime Agency, being lectured to about how some of the worst aspects of child pornography being transmitted around the world are dealt with. We do try to keep up with that.

But, no, you are making a judgment. In the new system, I have no doubt—and I disagree with Sir Mark here—that there should be one or two people with serious expertise in technology. I also think there should be a legal adviser. The law is extremely complex. RIPA is a dreadful piece of legislation. I say that with some strength of feeling, having had to try to understand it. Why do judges need a legal adviser? For that reason: to say it could be any one of 17 possible interpretations, rather than the five you thought you had. More importantly, in this system, from time to time you need advice. That is what I would like to happen, but then I envisage this as rather different from the bits and pieces you are seeing put together before you today.

Q53 **Lord Hart of Chilton:** You heard us discuss with Sir Mark the question of the judicial review principles that underlie the judge's oversight. I wondered if any of you would like to comment further on what he said. We were exploring whether it is right to call it a real double lock system. Are there any points you would make, further to the points made by Sir Mark?

Sir Stanley Burnton: Judicial review is not simply a question of looking at process. In the context we are discussing, the commissioner has to look at necessity and proportionality. The degree to which judicial review is imposed as a test and the stringency of the test depend very much on the context, the facts of the individual case and the consequences of the administrative or governmental decision in question. In the context we are discussing here, it is not unfair to describe the process as a double lock.

Lord Judge: That is rather my view. My only hesitation, which is a lawyerly one but not totally without some force, is in using the words "judicial review" as a description of the test that has to be applied by the judicial officer. Judicial review used to be Wednesbury unreasonable mad. We would call it Wednesbury unreasonable, meaning only an idiot could have reached this decision. Nowadays, judicial review is less stringent than that: "He is not an idiot, but it is a really stupid decision". That is not quite the same. "I am not sure many people would have reached this decision" is another test. We need to be slightly careful.

If you are talking about the Home Secretary, and I think you are, I have a separate point. There is a difference between national security warrants and ordinary criminal warrants.

What we do should be the system for ordinary criminal warrants: an authorisation in advance. That is a double lock. National security is rather different. The Home Secretary has the most amazing responsibilities in relation to that. Judges second-guessing is simply inappropriate. You have to have a stringent judicial review test. I am now coming back to what Sir Stanley said. You know you are dealing with national security; you know somebody might be planting a bomb. You are going to be very cautious about interfering and saying, "This man or woman, who is the Secretary of State, is daft". So I think the double lock system will work pretty well.

Sir Stanley Burnton: You can forget about Wednesbury unreasonableness in this context. Interestingly, proportionality and necessity are tests that we have imported from Europe, and the proponents of the Bill are clearly happy to adopt them in this context.

Q54 **Matt Warman:** As a still fairly new Member of Parliament, it struck me, observing the procedures of Parliament, that, if you have some pretty crazy procedures around for long enough, they become lauded as institutions. You described a pretty crazy set-up in your opening remarks, but does it not function as a sort of quadruple lock on what we have already, if you are constantly going back to ask for re-authorisation? I wonder what we are going to lose by streamlining it, if anything.

Lord Judge: I am sorry, I must have been unclear. They are not re-authorisations. Each one is a fresh authorisation by a different body. Sometimes the body will not even know what the earlier authorisation was. It is not a quadruple lock at all. Each is an individual one.

Matt Warman: So you do not see any strength from having three different people.

Lord Judge: No. I see potential for confusion. A much more coherent system would enable the same commissioner to look at one case. "This is the case of Snooks. This is the drugs ring. Right, the undercover officer has gone in. Here he wants this. Does the authorising officer think this is appropriate? Yes", and so on. The whole thing can be kept, in effect, under one person's eyes. It is much more proportionate. Sorry I was not clear enough. They are separate organisations.

Matt Warman: The argument that has been put is: at the moment, we have three commissioners, and, if one person makes a mistake, who is checking up? You would not accept any of that.

Lord Judge: People make mistakes, certainly, but we are all independent organisations. We talk; we discuss problems together, but we operate completely differently. It is not a system with the three sections of this keeping an eye on each other. We do not.

Q55 **Lord Butler of Brockwell:** When we took evidence from Home Office witnesses last week, they introduced a new concept, new to me anyway, of rationality. We asked whether reasonableness would be a test, and the witness seemed to dissent rather. He made a distinction between rationality and reasonableness. Is that a distinction you recognise?

Sir Stanley Burnton: The Wednesbury test is a rationality test: that no sensible administrator or executive correctly applying the law could have reached this decision. It is not a very stringent test; it is only in extreme cases that you are able to say something is Wednesbury unreasonable, whereas proportionality and necessity are more stringent.

Lord Butler of Brockwell: You are saying that there is no great distinction between reasonableness and rationality.

Sir Stanley Burnton: I am.

Lord Judge: I would not have noted any difference between them. I would not have argued the point with you. If you had said "Is it reasonable?", I would not have said, "It has to be rational".

Q56 **Stuart C McDonald:** I have a rather more mundane question about money, I am afraid. The impact assessment suggests that the new oversight and authorisation regime should cost around £150 million over 10 years. Would you regard that as realistic? If you do not feel able to answer that particular question, would you say that you have had sufficient resources to carry out your jobs fully, or are there other things you would have liked to do that you have been constrained in?

Lord Judge: I could give you a list of my complaints.

Stuart C McDonald: Please do.

Lord Judge: Our technology is, for obvious reasons, supposed to be secure. Our Brexit system—I am so sorry; I have something else on my mind—our BRENT system is hopeless, so we want it improved. We wait too long for new appointments to happen, and so on and so forth. Parliament has to decide how much it is going to spend on protecting the citizen from the threats of crime and terrorism, and how much it is going to spend on ensuring that those who should not be being surveyed in any way at all are protected from it. If you go down this route, you will have to have—I would strongly recommend if I were asked, so I will tell you anyway—a location separate from the Home Office, and people working there who are not drifting in and out of the Home Office. The perception of independence is strengthened by going to a separate place.

I mean no discourtesy; our rooms are pretty cramped. You are going to have a big system. If you have the same number of commissioners I have, which is six plus me plus three assistant commissioners, that is ten before you start. If Parliament enacts a system in which there is authorisation for everything in advance, it is going to take a lot more people. It will cost a lot more. We can either do it on the cheap or spend more money. We are in times of great financial stringency. I am sorry, but this is really not for me to say. I might say it in a different role, but not here. Yes, it will cost a lot more.

Sir Stanley Burnton: I am not an accountant and I cannot give you a figure. My impression is that in order properly to run the system, there are going to be something like eight judicial commissioners, which is quite a lot of staff. They must be backed up with appropriate staff, with the kind of skills my office now has but more widely available. There will be more inspectors, who must be appropriately qualified. You are looking at significant sums of money.

Incidentally, on a question that Sir Mark was asked, it ought to be the chief commissioner who determines what staffing and resources are needed. He must, of course, approach the Treasury and agree a budget, but it seems to me to be inappropriate for the person who is being monitored in a sense to be the person who decides on the resourcing of the office.

Indeed, internationally, one increasingly finds that judicial bodies are not subject to a Ministry of Justice, so far as resourcing is concerned. It is the judiciary that determines the resources it requires, subject to Treasury agreement.

Lord Judge: I entirely agree with that. The idea that judges will be looking at the Home Secretary's decisions and saying, "We do not think that is right", and then going cap in hand to that same Minister is not a sufficient separation.

Stuart C McDonald: That is helpful, thank you.

Q57 **Lord Henley:** I asked Sir Mark earlier about cost. This takes me on from Stuart's questions. Are you saying that under the new arrangements you should, almost as the universities used to in the past, negotiate directly with the Treasury without any intermediary?

Lord Judge: That would be my view. I make this clear: I am not seeking appointment to be the high panjandrum for this. A direct communication between the Treasury and the Commissioner is the way to do it.

Sir Stanley Burnton: As a matter of principle.

Lord Henley: Is that because your independence would be undermined if you had to go through the Secretary of State?

Sir Stanley Burnton: The appearance of independence is undermined if one has to go through the Minister whose work one is supervising.

Lord Henley: I ask that purely because I remember, back in the long, distant past, that that is how university funding used to be done when universities were independent. It is no longer the case; there is a department that looks after universities. That might be the way forward.

Lord Judge: In the context of the way the judiciary works, there has been coming and going about this, but I used to agree a budget or not agree a budget. I also had the power, which I never exercised, not only to write and say, "I do not agree it", but to say, "I am going public and this will not do". You need some kind of arrangement like that. We are both in the same place. If we are going to supervise the Home Secretary, we must not be answerable to him or her for the money.

Q58 **Lord Strasburger:** Would you be attracted to the system that exists in New Zealand, where the people in your position have a fixed percentage of the spend on intelligence and policing, and the decision is taken out of politicians' hands?

Lord Judge: The decision as to money?

Lord Strasburger: Yes.

Lord Judge: Ultimately, the Government have to find the money, so there has to be a discussion with somebody who represents the Government. Therefore, that is why we both say the Treasury.

Sir Stanley Burnton: I think I would need notice of that question.

Jo Cavan: If we went to that type of model, our percentage would no doubt be significantly lower than the percentage in New Zealand, because of the larger scale of our intelligence agencies, in particular the bulk collection we do, in comparison to New Zealand. Anyway, I do not necessarily think it is a bad model. I would say that the legal mandate and oversight provisions the New Zealand inspector general has are far more explicit and comprehensive than the ones in this Bill.

One of our points on the clauses around oversight is that they relate only to judicial commissioners; they do not relate to the commission. If we are going to create this world-leading oversight commission, it is important that the commission is explicitly referenced and the legal mandate, powers and functions are comprehensively covered.

Lord Strasburger: For the second time, I will say something about judicial review. I asked the Home Office on Monday why the words "judicial review" were in there, and they could not really tell us. What would be the effect, do you think, if they were struck out? Would the Bill be better for it, or worse?

Lord Judge: Parliament has to decide what function the judge is to exercise. Judicial review is a well-known series of principles, even though occasionally you hear it expressed in different ways. As I said a few minutes ago, in terms of national security, the idea of the judge in effect making the decision simply cannot arise. If a bomb goes off in London tonight, it will be the Home Secretary who will be down there. It will be she who has to answer to the House about what has gone on; it will not be the judge. We have to be careful to remember that there is a political responsibility, which is in the hands of the Minister, and we cannot dilute that.

Sir Stanley Burnton: If I remember rightly, the legislation on control orders, which are orders short of imprisonment to control people who are suspected to be terrorists, also requires the judge to apply a judicial review test. In practice, of course, in SIAC, the judge hears, often in secret, the evidence that is available to show that someone is a security threat. He applies quite a stringent test, because he has the information and knows whether there is something justifying imposing a control order. The legislation has changed, but it is not dissimilar.

Q59 **Bishop of Chester:** The fear in some quarters is that this new system will end up with rubber-stamping, that it will not be sufficiently independent. That is the fear abroad in some quarters. I am trying to imagine life in the increasing digital swirl in the years to come, with the exponential growth in communications and means of communication. How can we get some feeling of control and exercise oversight, and not simply be carried along in the tide? The threats in the 21st century will probably increase as well. Can you give us some idea as to how this double lock, this independent supervision, will work in practice?

Lord Judge: I hope I am not being discourteous. It is very easy to drum up anxieties. I am just as worried about criminals being able to get hold of information as I am about any of the authorities. We concentrate on the authorities. I do not know what is going on in this room even as we speak, but the technology available to serious criminals is, at the very least, as good as is available to law enforcement people. You trust your judiciary to make decisions against the state when it is appropriate to do so. I do not think anybody suggests that the judiciary nowadays is less independent than it was. In many ways, it is more so.

You have men and women who have exercised these functions all their professional lives, first at the bar or as solicitors, then as judges. They are men and women of proven experience and quality. You just have to work on the basis that you should trust them.

Bishop of Chester: Would it be better for perception, if nothing else, if the appointment of the commissioners was not made by the Executive. Just as you made those comments earlier about having clear blue water between the Home Office and this, would it be better to involve an agency more independent than the Executive?

Lord Judge: It is the Prime Minister's appointment. The Queen appoints the Lord Chief Justice, but that is on the recommendation of the Prime Minister. I do not suppose the Prime Minister spends a lot of time deciding what he is going to recommend to Her Majesty. There is, in the case of the judges, a Judicial Appointments Commission. I would not recommend that for these appointments. Apart from anything else, they have far too much to do and it takes a very long time.

For the very last commissioner who was appointed to my team—and this you could consider—a senior serving judge and a member of the Judicial Appointments Commission sat together, with my predecessor as an observer, and they chose whom it should be, and the appointment was then made. That is a perfectly sensible system. It is only theoretical that the Prime Minister has anything to do with it. It is very nice for me to be appointed by the Prime Minister, but I honestly do not suppose anything more.

Sir Stanley Burnton: By prescription, the commissioners are going to be either actual serving judges or former judges, and so one has to bear in mind that they will have been independently appointed, initially. Whether they will be full-time judges working part time as commissioners or are expected to be full-time High Court judges seconded to the commission, the Bill does not make clear. We probably both have concerns about the ability of the existing High Court to have people seconded to a different function, given that the High Court itself is under pressure.

Jo Cavan: Before we move on, I wanted to talk about the end-to-end process, because a lot of the debate has been focused purely on the double lock and the authorisation process in the first instance. Yes, that is crucial, but what is equally crucial is the post-facto audit functions, which look at the process from end to end. We carry out over 200 inspections a year and make over 800 recommendations to improve systems and procedures in compliance.

The inspectors, during their inspections, are looking at post-authorisation: was the actual intrusion foreseen at the time the warrant or authorisation was given?; has the conduct become disproportionate because the level of intrusion was not anticipated? They are looking at how the material that has been gathered has been used. Has it been used in accordance with the purpose that was set out in the warrant? They are looking at the retention, storage and destruction procedures for that material. They are looking at whether any errors or breaches occurred as a result of the conduct. All those post-authorisation functions are critical to ensure that you are overseeing and auditing the end-to-end process. That is where the modification and ongoing review of these provisions come in.

Sir Stanley Burnton: The reviewer will also look at the duration of the warrant and may go to the public authority concerned and say, "How is it that this warrant has been renewed twice? What evidence have you been gaining from it? Was there any justification for its continuation for such a long period?'

Q60 **Mr David Hanson:** In relation to Clause 176, which establishes the budget, as we have discussed previously, are you therefore suggesting to the Committee that we should consider recommending a rewrite of that clause that separates completely the funding from the Secretary of State, not just in terms of the effective micromanagement that the clause could imply, although in practice it probably will not, but in terms of the principle that the Treasury should be the lead department that you directly negotiate with?

Lord Judge: If we retain the present Bill in relation to judicial oversight of the Home Secretary, yes, unequivocally.

Mr David Hanson: I have a second point. Lord Judge, I noticed you made the point that it is very nice to be appointed by the Prime Minister, but you are sure he does not take much interest in it. I suspect, as many people in the past, should you be a troublesome priest, he may take some interest in your reappointment. I am wondering, given what the Lord Bishop has said, whether or not consideration should be given to independent appointment, rather than direct ministerial appointment, into the oversight role, given that oversight role?

Lord Judge: If we envisage that, 20 years from now, the Prime Minister of the day decided that he or she was not going to re-appoint somebody, and had no good grounds for doing so save that he or she did not like the colour of their face, or whatever it might be, there would be an absolute scandal. I really do not think Prime Ministers would want to get embroiled in that sort of thing.

We have to be careful about public perception, if you do not mind me saying so. Most members of the public, I suspect, want to know that those of us who have responsibilities in this field are seeing that the job is done efficiently, ie to protect them, and fairly, to protect their own rights. That is what they want. I do not think that they are going to be terribly fussed, largely, about whether the Prime Minister's name goes on the appointment, or whether it is that of the Speaker of the House of Commons or the Lord Speaker. One has to be careful. That is my view about it. If I were in charge and, the Prime Minister failed to re-appoint somebody and I thought this was the reason, I would go and see the Prime Minister and tell him, "I will go public about this".

The Chairman: Thank you very much indeed. It was a fascinating session and we are grateful to all of you for coming along. You have given us very interesting stuff to chew over, to say the very least. Thank you very much indeed.

Lord Judge: Thank you.

Peter Carter QC (QQ 186-196)

Evidence heard in public Questions 186-196

Oral Evidence

Taken before the Joint Committee

on Wednesday 16 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Lord Butler of Brockwell, Bishop of Chester, Lord Strasburger.

Witness: **Peter Carter QC**, gave evidence.

Q186 **The Chairman:** A very good evening to you. I am sorry that we are a little later than we thought, but we have had a couple of fascinating sessions. I have not the slightest doubt that this will be equally fascinating. You are all most welcome to the Committee. As you know, in these situations different Members of the Committee will ask different questions, but I am going to ask a very general one, which perhaps gives you an opportunity to make a general comment on the Bill that the Committee is considering, if you wish to. Aside from the new powers on the retention of internet connection records, in your view, does the draft Bill consolidate existing powers or extend them? In answering me, if you wish to make any more general comments, please do so.

Matthew Ryder: The answer to that question depends slightly on, when you talk about extending the powers, whether you mean extending what the security services and the authorities are already doing and what they say is authorised, or what others would say is currently authorised under the existing legislation. There is a dispute and lots of litigation about what is or is not currently authorised under the existing legislation.

My view would be that there are a large number of new powers that are not properly authorised within existing legislation. Just to go through them with headlines, in Part 1 of the Bill, thematic warrants are allowed in relation to Clause 13. There is not a thematic warrant provision for targeted surveillance and targeted interception within RIPA. I know that the Government say that, if you cross-reference Section 8(1) with Section 81, you can find group surveillance as part of targeting but, realistically, thematic warrants are something new, and the idea that you could target people as groups by their activity is something new in part 1 of the Bill. It is important because, conceptually, it is anathema to the existing culture of surveillance that has been going since the 18th century in this country. If we are to move in that direction, it needs an informed parliamentary debate about it, to decide if we want to go in that direction.

Secondly, mass surveillance or bulk interception—whatever you want to call it—under Part 2 of the Bill is essentially something new. I understand—I was involved in the case and litigated the case in the IPT last year—that the Government say that bulk interception or

bulk collection is permitted under Section 8(4), but there is a dispute about that. There is a case on its way to Strasbourg. It has been communicated in Strasbourg. There are many of us who would say that it was not set out very clearly, if it was permitted at all, in RIPA.

Part 5, on equipment interference, is really new. It has really emerged only since the draft code of practice was published in February 2015 in response to ongoing litigation. It turns out that the Government's position on the existing power is that it is a very broad power, under Section 5 of the Intelligence Services Act, combined with the draft code that they published on the door of the court in February 2015, so equipment interference is new. It is a very significant power that requires a lot of scrutiny and debate.

Part 7, on bulk data sets, is essentially new, has not been regulated before and is not in the existing legislation in any meaningful way. The power to have access to bulk data sets and how they would be defined is something new.

I missed Chapter 2 of Part 6 on bulk communications data acquisition. That is essentially new. In other words, the large collection of communications data in bulk is something that was not clear from any legislation before. That is essentially being regulated for the first time, under this Bill.

Finally, it is arguable—this is more debateable—that Clause 189, which is the clause that has tech companies particularly concerned, is if not new then certainly of new significance, because it requires telecommunications service providers to maintain their capabilities and combines that maintenance requirement that existed in RIPA with a new definition of a telecommunications service and those who are providing that service. It is broadened out by Clause 193(12) to those who are allowing those communications. That means that those companies that simply have communications apps that facilitate communications through the internet, such as Facebook, Apple or those sorts of companies, may be caught in a way of maintaining their capability that they had not imagined before. That opens up the question of whether encryption is engaged in relation to that issue and, if it is not in the Bill as it stands, in due course whether that is a concern. In summary, there is quite a lot here that is very new and these powers are important. They are significant and, therefore, because they are new, they would require debate.

Martin Chamberlain: That was a very comprehensive answer that enables me to be much briefer. The answer to whether and to what extent the Bill contains new powers is very difficult, for this reason. In the run-up to the tabling of the Bill a number of things that nobody knew the agencies were doing, they were revealed to be doing under the existing powers. There has not been time for some of the things that we have very recently found out the agencies are doing to be tested in legal proceedings. I am thinking there particularly about the use of the extended definition in Section 80 of RIPA effectively to enable thematic warrants to be issued, and the use of Section 94 of the Telecommunications Act 1984, which is something we found out about for the first time in the immediate run-up to the tabling of this Bill. As to whether those activities that we now know have been undertaken by the agencies are lawful under RIPA, the answer is that it has not been tested and so it is very difficult to know.

Generally speaking, whether the Bill confers new powers is, with respect, not a terribly helpful question. One of the important purposes of this Bill is to get a democratic mandate

for things that have not yet had a democratic mandate. Whatever you might say is the correct judicial interpretation of some of the old powers, certainly it can be said, without any doubt, that quite a lot of the things in this Bill are things that nobody in these Houses of Parliament has examined the justification for, to date. Are they new powers? One can debate that. The courts have not had the opportunity to debate it, in many instances. They certainly are new in the sense that they have not had a democratic mandate, in many cases.

Peter Carter: Needless to say, I agree with all that has been said, so I shall be even shorter, I think. This Bill is important, because it enables the democratic process to take control of what has hitherto, to a large extent, been a hidden exercise of what is known as a prerogative. It is about time that the prerogative powers were brought to heel and this is a good way of doing it.

Insofar as this Bill brings within the ambit of the law practices that hitherto have either been questionable or possibly outside the law, there is a huge amount to commend it. Only if the kind of activities that this Bill encompasses are subject to law and lawful control, and therefore lawful monitoring, can it be said that these powers are being exercised in a truly democratic way. We need the powers in this Bill, to some extent or another, to combat serious crime, terrorism and actions against the state. The exact extent is a matter for political debate, as well as legal debate.

One of the problems and one of the ways in which the current drafting of the Bill, potentially and exponentially, will extend the powers is in the definitions clause, Clause 195, which includes a definition of data. As Matthew has said, one of the things that appears to be an extended power is the bulk acquisition of data. Data is defined in Clause 195 as including any information that is not data. Therein lies a problem.

Graham Smith: I am going to be slightly longer. I have identified quite a few new aspects that are potentially new powers in this. First, although the question caveats out internet connection records, we do need to understand that, when one looks at Clause 71, which is the power to issue data retention notices, and one compares it with the existing data retention powers in DRIPA, as amended by the Counter-Terrorism and Security Act of 2015, and if one adds internet connection records to that, Clause 71 still goes far beyond adding internet connection records to the existing data retention powers.

Although this has been presented as something to enable the retention of internet connection records, it goes far beyond that in five or six different ways. Perhaps most significantly, the existing DRIPA powers are restricted to a few types of human-to-human communication—internet email, internet access and internet telephony. This would catch all the background activities on my smartphone that happen when it is sitting by my bedside when I am asleep, when I am away from it, whether it is receiving notifications, getting software updates or anything of that sort. It would capture and cover any machine-to-machine communication, which if you look forward to the internet of things would cover my connected home thermostat or my car checking if it needs a software update. Essentially, anything connected to the internet or indeed any other type of network would fall within Clause 71. It now applies to private services and systems, as well as public, and of course the power to require data to be generated for retention, not just retained, is completely new. The previous limitation to retaining data generated or processed within

the UK has been removed, so Clause 71 is very much broader than one might think by just referring to internet connection records.

Other new and extended powers are technical capability notices, under Clause 189. At the moment, under RIPA Section 12, capability notices can be given to support interception warrants and nothing else. Section 189 will apply also to all the new types of thematic, targeted and bulk warrants, under Parts 5 and 6, and will also apply to support the acquisition of communications data under Part 3. All of that is new.

In bulk interception, there is a new power. I call it a new power, but it comes as a result of the warrantry definitions; however, there is effectively a new power to extract related communications data from content and to treat it as related communications data. For instance, if I send you an email saying, "Here is somebody's email address", that is part of the content of my email, but the email address can be extracted from the content and then treated as related communications data. That is very significant, because most of the restrictions on examination of content do not apply to related communications data, so it is very significant. That is replicated as well in the new bulk acquisition and equipment interference powers, which talk about equipment data, which is more or less equivalent to related communications data. There is the power to extract equipment data from the content that is acquired in that way.

Lastly, there is the extension generally through the knock-on effects of the expansion of the definition of telecommunications operators in the draft Bill.

The Chairman: Thank you so much. They were some very useful answers.

Q187 Matt Warman: Given that we cannot agree on what is meant by new, I slightly hesitate to ask this. The Committee has been blessed with lots of different interpretations of what judicial review will mean in the context of this Bill. What do you think judicial review terms would mean, as far as the authorisation of warrants would go, in this new Bill?

Martin Chamberlain: You have just heard from David Davis about Lord Pannick's article in the *Times*, where he suggested that, in this kind of context, the judges would be applying a high intensity of review. One can explain it in this way: whenever a judge is applying a judicial review standard, there is a spectrum of different types of intensity of review. At one end of the spectrum, there is very light-touch review, which David Davis accurately described as, "Don't touch it unless it's totally barmy". Then at the other end of the spectrum, there is a real rolling up of the sleeves, getting into the detailed kind of review, where the judge comes close to substituting his or her own judgment for that of the ministerial decision-maker.

Practically any judicial review practitioner will tell you that, in practically any judicial review case, a key point of contention between the parties is where on the spectrum that case lies. Is it a light-touch case, is it an intensive-review case or is it somewhere in between? David Pannick's article in the *Times* suggests that this would be an intensive review kind of case. David Pannick is generally right about most things, but I would venture to suggest that you need to apply a bit of caution to whether that is correct in this context. Certainly it is true that a warrant authorising interception involves an invasion of someone's privacy,

but it does not involve the kind of restriction of liberty that you see in, for example, a control order case or a TPIM.

The Committee suspended for a Division in the House.

Matt Warman: You were in full flow on what judicial review is likely to look like in this context.

Martin Chamberlain: I have explained that there is a spectrum in judicial review, in terms of intensity of review, with very light-touch review at one end and high-intensity review at the other. David Pannick thinks that, because of the privacy context, we would be in the high-intensity part of the spectrum. I question really whether that is correct. The reason I question it is this: the matters under review, under Clause 19, are whether the warrant is necessary and whether the conduct authorised is proportionate. If you just concentrate on that second question, you are asking yourself the question as a judge reviewing this warrant whether the national security benefit to be derived from the warrant is proportionate to the intrusion into privacy that it involves. That is, to my mind, typically the kind of question on which judges will give a great deal of what used to be called deference—some of the later judgments deprecate that term, but leeway or latitude, however you want to put it—to the elected Minister. That is what would normally happen in judicial review. There is a House of Lords case called *Rahman* that makes that point. Where you are looking at proportionality assessments by a Minister who is accountable to Parliament, you apply a very light-touch review.

The touchstone, if you really wanted to get an interesting answer to this question of where on the spectrum it lies, is to ask someone from the Government what they think and see if they would be willing to give the kind of parliamentary statement that could be relied on in subsequent legal proceedings, to say that what they meant by judicial review was intensive review. I doubt whether you would get them to say that, because I suspect they would want to reserve the position to argue in front of the commissioners that it was a light-touch review that was intended.

Peter Carter: I hope Lord Pannick is correct, but I also fear that it is so uncertain that he may not be. This is not an area in which uncertainty can possibly be allowed to be sustained. One of the problems about judicial review is a problem that was created by Lord Judge last year because, in a decision called *Regina v L*, a decision in the Court of the Appeal in which he gave the judgment, L was somebody who as a young woman who had been trafficked for exploitation. The question was whether it was right that she should be prosecuted for an offence that she committed as a result of her exploitation, which we would now call modern slavery. The issue was what test is to be applied to the decision of the Crown Prosecution Service to proceed with her prosecution, even though all the circumstances demonstrated that she was a victim of exploitation. The test to be applied is one of judicial review.

There was the kind of discussion that we have heard about: on the one side this; on the one side that. Lord Judge said that we are going to apply in this case a test that is not the conventional judicial review; it is something different from that. The difficulty was that he did not say what it was. I do not know anybody at the Bar, who practises in that area of

law, who understands what the test with which we are left in that area of law is. What I suggest is that the simplest way of removing this ambiguity is to suggest an amendment that you simply delete the words about judicial review.

May I go back to the stage about how the judicial commissioners will consider this? It starts off with reviewing what? A decision by the Secretary of State. Normal judicial review is a review of a decision and the reasons for that decision. Are those reasons irrational or are they rational? Do they include considerations that are immaterial or are they centred on considerations that are central to the issue in point? I do not think there is any provision in this Bill for the Secretary of State to give reasons for his or her decision. The judicial commissioner will not be reviewing reasoned decision. The judicial commissioner will be reviewing the decision and, therefore, ought to be reconsidering from scratch whether or not it is appropriate to authorise this warrant and doing so by applying the test of necessity and proportionality.

There is one slight twist about this because, by Clause 169(5) of the Bill, "In exercising functions under this Act, a Judicial Commissioner must not act in a way which is contrary to the public interest or prejudicial to … (a) national security, (b) the prevention or detection of serious crime, or (c) the economic well-being of the United Kingdom". I cannot imagine for a moment that any judge or judicial commissioner would act in a way that is contrary to the public interest, but who is to determine and who is to assist the judicial commissioner on what is national security, what is in the economic wellbeing of the United Kingdom, particularly if the judicial commissioner is not assisted by reasoning from the Secretary of State? If there is to be reasoning from the Secretary of State, how long is this process to take and why not simply remove the Secretary of State from the process?

Matthew Ryder: May I just make two very short points on this? The first one is that the role of the judge in judicial review, when it has been explained, might be slightly confusing in the sense that there is talk about deference. The question might be what the judge would add in making a decision, if he is going to be so deferential. That is to do with the role the judge has in judicial review, versus the role that the judge would have if the judge was having to authorise it themselves.

I have drawn an analogy here, because it goes back to some of the discussion we overheard from the previous session. There are times when this conversation seems as though it is discussing the difference between political accountability and judicial accountability. One has to remember that the authorisation, in this process, is one very small part of an overall operation, the vast bulk of which is not decided by the Home Secretary or a politician, but is decided by police and judges.

For example, Schedule 5 to the Terrorism Act which is the part that controls terrorist investigations, contains a large number of provisions, production orders and search warrants, including producing material from journalists, all of which are decided by a judge. Those can be much more intrusive, in some circumstances, and much more serious than intercepts, but we trust that to the judge. In serious crime operations, we trust search warrants and production orders to a judge, for a judge to make that decision. The judge does that not by deference to a ministerial decision but by having their own role in terms of making that decision for themselves, and it is a system that works very well with serious crime and under Schedule 5 of the Terrorism Act. That is why one can be led down a

cul-de-sac in thinking that we are choosing here between a brand new type of judicial authorisation or judicial role, when previously it had always been the Home Secretary. In reality in terrorist investigations and in serious crime, it is judges and police who are having to make those decisions and who are accountable for those decisions—sometimes life and death decisions.

Q188 **Victoria Atkins:** I should declare that Peter Carter and I were in chambers together. Mr Carter, you have talked about there not being any provision in the Bill that you can identify for the Secretary of State to give reasons. I have to say, listening to that, I thought, "Crikey, this is a lawyer's paradise". Is it not? We heard from Mr Davis earlier. He estimated that there are 2,300 intercept warrants a year that the Home Secretary does, which equates to nine a day, in addition to all their other duties. If the Home Secretary is having to sit down and write out reasons, in the way that you and I understand as lawyers, I fear that would be a real burden, adding bureaucracy in what is a highly dynamic environment. Is it not better to look at the evidence from the security services or whoever is making the application? Look at that and then the judge looks at it again—the same evidence—and makes their decision according to the evidence placed in front of them by the security services.

Peter Carter: I entirely agree. We do not want this to be a lawyers' paradise. It is going to defeat, not assist, the end. If the law is clear, there is less room for lawyers to get involved. You do not want lawyers getting involved to try to disentangle what ought to be a clear and transparent process for those who need to know about it. My only slight difference of opinion with what you suggested is I do wonder whether the Secretary of State needs to be involved at all, other than in those things that involve the security services.

Q189 **Suella Fernandes:** I have a question; I think Peter and Martin dealt with judicial review. We have heard evidence from Lord Judge and Sir Stanley Burnton, who have stated that they think it does strike the right balance, but proportionality involves a balancing exercise—a consideration of the objective and whether the objective is sufficiently important to justify the intrusion, whether the measures are directly related to the objective and ensuring that it goes no further than what is necessary. Do you not think that that encompasses a very clear and balanced assessment of the decision to issue a warrant?

Peter Carter: I do and those words are perfect, provided they are left alone.

Martin Chamberlain: I have to say that I am not quite so sanguine that the word "proportionality" necessarily connotes a high-intensity review. Within the case law on proportionality, under the Human Rights Act for example, there is still a very broad spectrum of intensity of review and, sometimes, even though the court is looking at proportionality, it gives the decision-maker considerable latitude. In other contexts, it gives the decision-maker rather less latitude.

The problem with simply saying that the standard to be applied is judicial review is that we do not know what arguments the Government will make to the judicial commissioners, and it is quite possible that the Government will say that this is the context, balancing the needs of national security against the intrusion into privacy, where you have to accord considerable latitude and discretion to the elected Minister, and where the judge really should not interfere, unless the Minister has obviously struck the wrong balance.

Suella Fernandes: Just by way of follow-up, would you confirm for the record that, in the process of judicial review, a judge would have access to the same information that was before the Minister throughout the original decision-making process? Is that your understanding of judicial review?

Peter Carter: Victoria Atkins made the point that this is a dynamic process and I entirely agree it is. Given the reality of the situation, particularly if it is a security service application for a warrant, it may well be that, by the time it gets to the reviewing judicial commissioner, which may be 15 minutes or half an hour after the Secretary of State has made a decision, further information is available. The judicial commissioner must take account of all the information that is then available, just in case there has been a shift—either augmented information or something that turns out to need correcting.

Q190 Lord Butler of Brockwell: When Mr Carter read out Section 169(5), saying, "In exercising functions under this Act, a Judicial Commissioner must not act in a way which is contrary to the public interest or prejudicial to—(a) national security, (b) the prevention or detection of serious crime, or (c) the economic well-being of the United Kingdom", I thought to myself, "Crumbs, that really is going to shackle the judge". It is certainly putting pressure on him to approve the warrant, but then I looked down and Section 7 says that that subsection does not apply "in relation to the functions of a Judicial Commissioner of—(a) deciding whether to approve the issue, modification or renewal of a warrant or authorisation". Perhaps you did not intend to mean that it was going to shackle the commissioner.

Peter Carter: No, I do not think it is. What I was concerned about was any suggestion, as perhaps had been made by one of the previous witnesses, that judges were going to be bowled over by a suggestion that this is for national security and, therefore, you must not intervene. The point is that the fact it is there will not prevent the judges from having a rigorous and robust appraisal of the information that is before them, before they make an authorisation or not.

Lord Butler of Brockwell: You are saying that this does not shackle the judge. It will enable the judge to reach full discretion.

Peter Carter: I think so. I hope that the reference to "contrary to the public interest", in any circumstances, would not be something that a judge would find difficult to understand.

Matthew Ryder: I was just going to say, in relation to the point you are making and the point made by Ms Fernandes, it is important to bear in mind that a judge in this position may have access to material, but a judge is not making his own assessment of the facts in judicial review. In the situation where a judge is assessing a search warrant or a production order in relation to something very sensitive, like Schedule 1 to PACE, which could be obtaining material from a journalist, or Schedule 5 to the Terrorism Act, which could be very sensitive and very serious, a judge has the evidence but then assesses that evidence. If the judge thinks the evidence is not sufficient, he could call for more or could look at it.

In a judicial review situation, the judge is essentially bound by decisions and assessments of facts that have been made by the Secretary of State and is applying judicial review principles—which, as Martin rightly says, can be on a range of scrutiny—to that assessment that has already been made of the facts.

The final point to bear in mind is that, normally in judicial review, there is an element of an adversarial process. In other words, the judge is assessing it with somebody making representations in relation to the other side. There will be no adversarial process built into this, the way it stands at the moment. You will have a judicial review, but no one putting forward the argument to the judge in a different situation. Now, that is not unheard of; you have that in other situations, but not in relation to a judicial review situation. That is why it is so important, in this sort of situation, for the judge to be able to be hands-on to potentially look at the facts and evidence in front of the judge, for themselves, and make that decision not shackled by any previous assessment that has been made by the Secretary of State.

Suella Fernandes: Do you not think that that will have a negative effect on timeliness and the speed of decisions, in urgent situations when there are real risks, in terms of the quality of decision-making?

Matthew Ryder: It should not do at all. The reason is that it does not have any problem with timeliness in relation to Schedule 1 of PACE. Those can be extremely urgent applications for very sensitive material in the most intense operations. It does not have any problems in relation to Schedule 5 of the Terrorism Act. I could not imagine a more serious situation, where a judge is having to decide on production orders or search orders in relation to terrorism investigations, under Section 39 of the Terrorism Act 2000, which are then being dealt under Schedule 5 of the Act.

Q191 Lord Strasburger: Not only am I not a politician, I am not a lawyer and I have been struggling through the fog of arguments in this area, since this Committee started to sit. It is only just now that I am beginning to see some light at the end of the tunnel. Are you collectively saying that the solution to this whole problem is to strike out the phrase that includes the words "judicial review"?

Peter Carter: Are you asking four lawyers to agree?

Lord Strasburger: I will settle for your individual opinion.

Peter Carter: My opinion is yes.

Martin Chamberlain: Mine is, too. It would be much clearer if you said to the judicial commissioners what standard you are expecting them to apply. You could do that in various ways. One way would be to get rid of the words "judicial review", which imply this shifting spectrum, without telling you where on the spectrum you are.

Matthew Ryder: I would still be inclined towards judicial authorisation by a judge, rather than judicial approval. I certainly think in relation to police cases that "judicial authorisation" would be appropriate. In national security cases, you can have a different discussion, but my preference would be "judicial authorisation", rather than "judicial approval".

Graham Smith: I am a mere IT and internet lawyer. I would not begin to venture an opinion on this.

Lord Strasburger: May I then ask the opposite question? What do those words add to the Bill? What benefit do they bring, if any?

Martin Chamberlain: The suspicion or the worry is that it may be argued by the Government, once this Bill becomes an Act, that what they add is a clear signal or flag to the judicial commissioner that, when you are examining warrants issued by an elected official, you should back off and not question those warrants, unless the decision to issue them was irrational or something close to irrational. Probably "irrational" is the wrong word, because clearly proportionality comes into it but, at the far end of the spectrum, that is the worry. It would be very interesting to hear what the Government say in response to that. If they were to say, very clearly, "That is not what we intend. We intend it to be intensive review", and if they were to say it in a way that could then be subsequently relied on in legal proceedings, that would be very interesting.

Q192 Dr Murrison: We have moved quite a long way towards the double lock. The double lock was a point of some controversy, but has now been accepted by the Government. It is worth just recording that. What you are saying is that you would be happy with the deletion of Clause 19(2), which we heard, for example from Liberty the other day, would materially improve the Bill and the scrutiny available.

May I press you on this five-day period, during which the judicial commissioner would take a view, albeit in the Bill at the moment a rather limited view, on the authorisation that the Secretary of State has given? Do you feel that five days is reasonable, since we have heard from others that it is a very long time for a judge to form a view, particularly since he is likely to be presented with the same sort of material that the Home Secretary deals with, sometimes with a very short timeframe? Indeed, that of course is used as a justification for the Home Secretary dealing with this in what have been characterised as emergency situations, not a judge. May I start? This is something that the Bar Council is particularly concerned about. We can see no justification for that five-day gap. The Secretary of State is a single person. Numerous judicial commissioners can be appointed and, no doubt, will be appointed under the Bill. High Court judges are used to dealing with applications of the utmost urgency.

When there is a need for an urgent application, for example a place of safety order or to prevent somebody being deported from the United Kingdom, I am afraid judges used to be wakened at any time of the day or night and can deal with that matter, as a matter of urgency. There is no reason why a judicial commissioner cannot deal with it as a matter of urgency. For example, a judicial commissioner might be in a position, as the Home Secretary probably might not, under the Bill, to say, "Yes, I authorise this warrant and I want you to come back in 24 hours and I will review my decision and how far it had got". There is provision for that in the Bill, but I can see that practice would develop whereby a judge would make an authorisation that was interim and conditional. I cannot see any reason why five days for a warrant that is potentially unlawful can be justified.

The Chairman: Can you suggest a time?

Peter Carter: I do not think there is any justification for any time, any delay. The delay, if anything, is going to be with the Home Secretary, not with the judicial commissioner.

The Chairman: The issue is one of urgency here, is it not? These are only urgent warrants. We are not talking about the 2,500 to 3,000 warrants that have to go through the various Secretaries of State. We talk about a much smaller number. Would that make a difference in terms of, I do not know, a day afterwards?

Peter Carter: The difficulty about that is that, if it is urgent, you should not prescribe a time limit because, if it is urgent, it must be done immediately.

The Chairman: Indeed, but the issue is if there is a joint authorisation, which there is on a normal warrant, but an urgent one, because of its very nature and what might be happening, the Secretary of State obviously has to authorise. The Bill says you can have up to five days for a judicial commissioner to review that, but you do not think there is any need for any sort of time limit. It depends on the availability of the judicial commissioner, presumably.

Peter Carter: There will be a judicial commissioner available at all times. There should be. It may well be that, if it really is urgent, the Home Secretary or the Secretary of State should be, as it were, a bystanding participant and it should be a single, consolidated process.

Matt Warman: How does that work?

Paul Hudson: The principal decision-maker and authoriser would be the judge. It would be subject to the Home Secretary saying, yes, he or she confirms that it is necessary, so you do it the other way round, in a sense.

The Chairman: To put in my own experience, from when I used to authorise warrants as a Secretary of State—very urgent ones, virtually in the middle of the night or something—you are not going to sit there and have to phone up a judge immediately, when something might have to be decided in minutes, surely.

Peter Carter: That is why I am suggesting that the only reason for having the Home Secretary's decision is this double lock process, is it not? The presumption is that the Home Secretary is a politician who is attuned to security needs and would be the first port of call but, in urgent cases, there is no need for that. The first and only port of call is the judge. If the Home Secretary, having been informed of the information says, "Actually, I disagree", which is highly unlikely, the Home Secretary would then have the power to revoke it.

The Chairman: Why are you suggesting that it should go to the judge before the Home Secretary in an urgent case?

Peter Carter: It is because you then have the consistency of every such warrant having judicial approval.

The Chairman: I understand.

Q193 Bishop of Chester: Is it possible to try to situate this whole discussion between the European culture, which has experienced totalitarian Governments and has a suspicion of government with the history of totalitarian interference, and North America, where there has always been that freedom of the individual and a small state. We are somewhere in between. There is a danger of these wide-ranging powers, which you have identified, being accepted

too easily, hence the need for some sort of robust double lock and a strong culture of judicial independence in the judicial element, I suggest. One of the questions we have raised is if the judges should be appointed by the Prime Minister or by the Judicial Appointments Commission. Should they be appointed for a single term of office, rather than have to submit to reappointment? There are these sorts of questions. Are there other ways of strengthening that culture of independence that you all want to see in the judicial involvement?

Peter Carter: Given the gravity of the kind of situation that is envisaged in this Bill, I would have thought that the appropriate candidates for judicial commissioners are likely to be High Court judges. It may be that it is because we have all gone native in the profession that we see no reason to doubt the integrity and the robustness of people who satisfy the criteria of appointment to the High Court bench. I do think, though, that there is a potential problem of perception, if not reality, if appointment to the judicial commission is by the Prime Minister, rather than by the Judicial Appointments Commission, with consultation with the Lord Chief Justice. That would be more appropriate, rather than it looking like a political appointment.

Bishop of Chester: Would you review after three years, as is proposed, or is it better and more of a culture of independence to appoint for a single longer term?

Peter Carter: I am not particularly bothered. Others may take a different view about that but, if you are appointing somebody of the category I have suggested, either they will be sitting senior judges, in which case after three years they may go back to their normal judicial appointment; or they may have retired, in which case three years would probably be sufficient for them to feel that they have done their job and would quite like to go and do something else. Potentially, it will be quite an onerous job. For somebody in this position, I do not see that there is a problem about the perception of independence from it being a three-year term, in the same way as, for example, for the appointment of the Director of Public Prosecutions, the term is sometimes three years and sometimes five years. Nobody, so far as I am aware, has made any suggestion of lack of independence as a result of a three-year, as opposed to a five-year, term of appointment.

Matthew Ryder: Three years is a short tenure for a judge and it might be that the Judicial Appointments Commission would be well placed to express a view about that sort of time in relation to judicial independence, because they have done some significant thinking on how long tenures should be for judges, to ensure that judges do not feel vulnerable when they next come up for review.

Bishop of Chester: When they appeared before us, the impression given by the judges was that they generally sided with the application. David Pannick's article referred to that benefit of the doubt or margin of discretion or whatever it was he said. I cannot remember the term you used there. One can see that a certain culture of it being normal to go along with the Executive could develop without quite being noticed. I simply put this up for you to demolish. Others who have sat in those seats would certainly have those anxieties.

Peter Carter: All you have to do perhaps is look at the history of the current Investigatory Powers Tribunal and the independence that has shown in standing up against the Government's attempts to keep secret the unlawfulness of some of the conduct, and the tribunal's insistence on making public as much of its judgments as it possibly can.

Martin Chamberlain: I would agree with that. I do not think you need to worry that the people who are appointed to these rules will slip into a culture of doing what the Executive want. What you need to worry about is that judges, in performing their role, will do what they think Parliament has told them to do. If they think Parliament has told them, by use of words like "judicial review", to accord considerable latitude to a constitutionally accountable Minister, then that is what they will do. That is not because they are unable to stand up to the Executive; it is because they are honestly interpreting what you have said to them. If you do not want them to apply considerable latitude, you need to make clear that they are not to do so. If you make that clear, they will do what you say.

Q194 **Victoria Atkins:** Lord Chairman, I am very conscious that I am about to venture into a subject in which you are an expert and I am not, but it is a simple question. Have you taken into account the political sensitivities of Northern Ireland and the way the judiciary is viewed by some, in different parts of that part of the country, when assessing the argument that judges should always come first?

Peter Carter: No.

Martin Chamberlain: I have not either, but I would have thought that, if and to the extent that there are elements of the community in Northern Ireland who have less confidence in the judiciary than perhaps people would have in England and Wales, or Scotland, then one would have thought that those same elements would have a similar lack of confidence or even a greater lack of confidence in members of the Executive.

Dr Murrison: I have a very quick supplementary to that. Do you think then that that is another argument in favour of the Judicial Appointments Commission appointing commissioners, rather than the Prime Minister? If the Prime Minister appoints the judicial commissioners in relation to Northern Ireland, one would also have to involve the First and Deputy First Ministers.

Peter Carter: I first heard that argument raised at a meeting in Portcullis House on the eighth of this month, and it struck me then that I wished I had thought about it before. It seems a very good suggestion.

Q195 **Suella Fernandes:** The Home Secretary will have the power to amend the functions of the judicial commissioners. How do you envisage that power being exercised and what kind of modification might be envisaged?

Matthew Ryder: I do not know is my answer.

Martin Chamberlain: I would say the same. It is very difficult to envisage how it might be exercised. In principle, it could be exercised to add to the functions or to take away from the functions. One potentially worrying use of the power would be if it could be used to alter the test that a judicial commissioner has to apply when considering or reviewing the issue of a warrant. I do not know whether it is intended to use the power or that the power might be used in that way, and it would be an interesting question to get the Government's view on.

Peter Carter: Can I make a suggestion? It seems to me that the power to modify the commissioner's role should be confined to those roles that are not central to the authorisation of warrants and the continuation or renewal of warrants.

The Committee suspended for a Division in the House.

Peter Carter: I am very grateful for that, because it has allowed me to find my place in the notes. The question was about the Home Secretary's power to modify the role of the judicial commissioner, which appears in Clause 177. In the clause as it stands, there are no constraints as to which role or part of the role the Home Secretary can amend. This means that, if you decide to remove the expression "judicial review", the Home Secretary could, by his or her power of amendment, depending on who it was at the time, put it straight back in again, which may not be entirely satisfactory.

This provision, Clause 177, appears in part 8 of the Bill. There are various provisions there that explain or provide particular functions for commissioners, including that the investigatory powers commissioner in Clause 169 must keep under review the exercise by public authorities of statutory functions, and so on. I can understand why that kind of role or function is suitable for amendment, as circumstances and the law change. What I would suggest is that Clause 177 should be amended by adding the words, in subsection (3), "This clause does not apply to any function of the judicial commissioner under parts 1 to 7 of this Act".

Q196 **Victoria Atkins:** I am conscious of the time. Mr Carter, you have written a very helpful paper, on behalf of the Bar Council, regarding legal professional privilege or LPP. Can you help us with any concerns about LPP and investigatory powers and, if there are concerns, how they can be addressed? How would you recommend they be addressed?

Peter Carter: We have concerns, because there is nothing in this Bill that protects legal professional privilege. Legal professional privilege is the privilege of a client to have private communication with a lawyer, to obtain legal advice or for advice and assistance in the course of litigation, whether active or potential. Communications between a lawyer and a client are not all protected by legal professional privilege, and we are not suggesting that all communications between a lawyer and a client should be protected or immune from investigatory powers. For example, the Proceeds of Crime Act makes it quite clear that communications between a lawyer and a client covered by legal professional privilege are immune, but a client asking a lawyer for advice on where the best place is to stash his stolen loot is not. If there was information that led the police or the security services to believe that that conversation was about to take place, then they would be fully entitled, and I would applaud them, for putting in place some of the provisions of this Bill to get evidence that that was taking place.

The difficulty is that, if legal professional privilege, properly so-called, is not recognised as a privilege that needs to be protected, it strikes at the heart of our judicial system, not just the criminal system, but the judicial system. It is the integrity of the judicial system that is one of the guarantors of our state as a democracy.

Imagine the situation if a client in a commercial action were to say to me or one of my colleagues, "I am about to engage on a contract and I need your advice as to the international effects of this. It is with a Russian company. It is very sensitive because I have competitors in other states. Can you assure me that all our communications will be confidential?". Under this Bill, my answer would be, "No, I cannot", because I simply do not know.

The difficulty is that the wording used in Clauses 5 and 65 says that, where a warrant authorises any of the investigatory powers under this Bill, then any action taken in accordance with that warrant is lawful for all purposes. If the warrant authorises the interception or the gathering of data information concerning communications between me and the client, it would be lawful, even though under international law, European law and our historic law, such communications have been immune, as a matter of public interest. The fact that these rights are ancient is neither here nor there; what matters is that they are current and they are important. They are important for the confidence of citizens in the administration of justice.

Interestingly, when David Anderson produced his report, *A Question of Trust*, in a fairly short passage, he described why legal professional privilege is important. He said, if it is apparent that there is no guarantee that legal professional privilege is protected, it will have what he called "a chilling effect" on the relationship between client and lawyers, and their confidence in the entirety of our judicial system.

The Government fight fiercely for its own legal professional privilege, particularly for example when it is engaged in international arbitration. The Belhaj judgment in the Investigatory Powers Tribunal said this, "There was no dispute between the parties", that is between the state and Belhaj, "as to the importance of protecting and preserving the concept of legal and professional privilege". Why, therefore, is that recognised importance not reflected in the Bill? It is in various other statutes, including in the Terrorism Act 2000 and in the Proceeds of Crime Act, as I have already identified, and in the Police and Criminal Evidence Act.

The problem is that there was one clause, in the Regulation of Investigatory Powers Act, Section 27, that used that expression, "lawful for all purposes". The House of Lords by a majority decided that that empowered a warrant to enable the investigating services, police and intelligence services to intercept communications covered by legal professional privilege between a lawyer and a client. In fact, what was uncovered out of that was of precious little significance, but it was a chilling effect. It has had a chilling effect. Those of us who practise sometimes in criminal law realise that what you require is to build up the confidence of a client in order to give robust advice, sometimes advice that they do not want to hear, but they need to hear. If they cannot be confident that the communication is confidential and secret, they will simply say nothing. That does not help anybody or anything.

Why is it not there? It is said by the Home Office that it is all right; it will be in codes of practice. Interestingly, Schedule 6 contains the only reference to something akin to legal professional privilege, and it is in paragraph 4 of Schedule 6. It says, "A code of practice about the obtaining or holding of communications data by virtue of part 3", so it is confined to the powers exercised under part 3, not under any other part, "must include … (b)

provision about particular considerations applicable to any data which relates to a member of a profession which routinely holds legally privileged information", which I assume means lawyers.

There are two things that follow from that. The first is that it recognises, as is evident from the proceedings in the Investigatory Powers Tribunal, that the security services have access to sufficient information to be able to filter those communications that are communications with lawyers, so they know which communications are likely to trigger access to data or communications, which are or the subject matter of which is covered by legal professional privilege. They can do that.

Why is it that the codes of practice under paragraph 4 of Schedule 6 are confined to this particular area under Part 3? The codes of practice or the draft new codes under the Regulation of Investigatory Powers Act also have a provision about legal professional privilege, which does not guarantee the immunity of legally privileged material from access by and disclosure to the agents of the state. It simply says it is a serious consideration, before authorisation is given, not only when it turns out that legally privileged material has been accessed inadvertently, as part of a more general and legitimate operation, but even when it has been specifically targeted.

Whether that will survive a challenge in the European Court of Justice or in Strasbourg, I have my doubts. I am not certain about it, but I have my doubts and I have my doubts because, in international and in regional human rights law, one of the critical basic rights is the right to independent advice or advice from an independent lawyer. Advice from an independent lawyer is going to be worthless if the client and the lawyer believe that everything said is going to be heard by or accessed by the state.

The state, in the cases that are dealt with in the Investigatory Powers Bill, will in most cases, the chances are, face some kind of litigation involving not necessarily the person whose communications are accessed, but somebody else. Eventually, the chances are, the litigation, whether it be criminal or civil, will indeed be between the person whose communications are accessed and the state. The state would not want to be at a disadvantage if another state in international arbitration had access to all its advice. There have been various expressions about the importance of this right over the centuries but, as I say, what matters is its significance now as a right in a democratic society, which is regarded as a guarantee of a democratic principle and a guarantee that citizens are not at a disadvantage in their dealings with the state.

The Chairman: I shall have to curtail things in a second. I am just asking whether your colleagues agree with what you have said on this or have any additional points.

Matthew Ryder: I do not have anything to add.

Martin Chamberlain: Neither do I.

The Chairman: There is no dissention, which is very good. I am going to close the session now. We have, however, a number of questions we would like to put, if that is okay, to all four of you, in writing. I am conscious of your time, but I am also conscious of the fact that I do not particularly want these questions or the answers to them to be missed. If that is okay

with you, we will write to you. We are very grateful. It has been a fascinating sessions and a very important session for this Committee. Thank you so much for coming.

Jo Cavan, Head of the Interception of Communications Commissioner's Office (QQ 47-60)

Evidence heard in public Questions 47-60

Oral Evidence

Taken before the Joint Committee

on Wednesday 2 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Stuart C McDonald MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Bishop of Chester, Lord Hart of Chilton, Lord Henley, Lord Strasburger.

Witness: **Jo Cavan**, Head of the Interception of Communications Commissioner's Office, gave evidence.

Q47 **The Chairman:** Lord Judge, Sir Stanley and your staff, thank you very much indeed for coming along to us this afternoon. As you know, this is a very important Bill. The Prime Minister described it as the most important of this Session. Much of the Bill refers to the change in oversight provision, so we are very grateful for your coming along. I wonder whether you want to say anything yourselves before we start asking some questions.

Lord Judge: I would like to say something, particularly in view of the discussion that has been going on with Sir Mark. I cannot think that anyone would have designed the present three-bodied system. It would never have happened; it should not have done. We work piecemeal on the legislation; we produce piecemeal results; and we have produced three bodies, all of which have responsibilities in the broad sense that we are talking about and all of which work in different ways.

Let me give you some "for instances". Sir Mark has just given evidence to you. He is the commissioner. He has no inspectors. Sir Stanley will tell you that he is the commissioner and, with his team, he has 10 inspectors. I will tell you that I have taken over the surveillance commission. I have seven inspectors, who are former police officers of no less than superintendent level, a Chief Surveillance Inspector, six commissioners, three assistant surveillance commissioners and, good heavens, there is even me. We all operate differently. The focus so far has been on Sir Mark, and I know that IOCCO, as it is called, has had quite a lot of input, but can I just explain to you how this leads to confusion and can be improved?

The Chairman: Please do.

Lord Judge: We have had to take on oversight and prior approval of undercover police authorisations. We all know about the relatively recent disasters caused by officers going wrong in undercover operations. There is an application to us and, mark this: we have to authorise. Neither of the other two Commissions authorises. Every single piece of intrusive

surveillance, certain types of property interference and long term undercover operatives for which we are responsible is authorised in advance by a commissioner, who is a former judge.

The case is made out to us that there should be an undercover police officer in this particular, rather serious drugs case. The authorisation is made. In goes this brave young man or woman—and most of them are very brave young men and women—and they discover that there is quite a lot going on and it would be a good idea to have some intrusive surveillance, say into a car that is being used to transport the proceeds of drugs. He has to go back to his authorising officer. The authorising officer comes to us, and there is another application for intrusive surveillance to take place. That takes place, and that reveals something else: these drugs are actually to do with a potential terrorist ring.

That does not come to us; that goes to Sir Mark, but there is no pre-authorisation by him. Somebody says, "We had better have some communications input". That goes to Sir Stanley. There is no pre-authorisation by him. Now, I am sorry to say this, but telling the story the way I have is entirely accurate. If you thought about it, you would say, "Is this really the way we are doing business?".

Speaking only for my own team, every authorisation is made before any of the aforementioned intrusion takes place. The papers come to us, and I have a complaint about the quality of our equipment, but that is another question. A judge commissioner looks at them. He decides whether necessity is established and whether it is proportionate, which involves looking at the nature of the offence. You would not authorise intrusive surveillance for somebody who was stealing a tin of salmon from a supermarket. You are looking at sentences starting in the three to four-year range and upwards. He checks for proportionality: is this a reasonable way to go about sorting this problem out? He authorises or does not, or says, "I want more information". Then the process goes through.

At the other end of the process, every year my inspectors go in and conduct an inspection of every single police force in the country, Her Majesty's Revenue & Customs and so on—all the law enforcement bodies. They conduct random analyses inspections of all the things for which the body is responsible, such as encryption. There are all sorts of different things that come under the remit of covert surveillance. They then write a report. The report is written to me. It goes to the chief constable. I write my own report to the chief constable. Sometimes I say, "This is being very well handled. Your authorising officers are well trained. The paperwork is very good. The explanations are excellent", and so on and so forth. I have just written a very rude letter saying, "This is not good enough. You are not complying. There are too many breaches. There is too much inefficiency in this part or that part", or whatever it is.

I write that to the Chief Constable, and then I go and see him, or one of my commissioners does. I go to all the big Forces. We discuss the report for the year. Most of the time—and this I hope does not surprise you—the chief constables are as anxious as we are that the job should be done properly. Apart from the reputational matter, they are men, and women now, who want the job done lawfully. They are also aware of the dangers of evidence being excluded at the trial process or an abuse of process argument leading to the whole prosecution being discontinued. I go there; we discuss it. If I am unhappy, I will go again. I have not had to, but I have only been in this job for a relatively short time.

I am not recommending it to you, but our system is very different from the one you have been discussing with Sir Mark, and from Sir Stanley's. The idea that we should have a surveillance system in which there are three different bodies is itself absurd, and then three different bodies operating differently strikes me as daft. That is my opening statement.

The Chairman: Very interesting it was, too. Sir Stanley, do you want to make any comments?

Sir Stanley Burnton: As you know, I am the new boy on the block. I have the good fortune to have staff who have received a glowing report from David Anderson, as you will have seen. They have a range of competencies, including computer abilities. There were questions asked of Sir Mark about training. I have some computer knowledge; I was judge in charge of IT, but I could not go into a public authority and interrogate their computer system. We have inspectors who can and do just that.

We carry out an audit function. I believe that you cannot carry out an audit function properly unless you have some understanding of the business you are auditing. That does not mean to say you could do it yourself. I could not go into a computer and interrogate it to see how many search or interception warrants had been issued, and view the grounds and so on. But I like to think I have a sufficient understanding of what staff can do, and do, to carry out the functions of my office.

Like Sir Mark, as far as I am aware, there was no special security clearance carried out when I was appointed. On the other hand, when I was a judge, I used to do Special Immigration Appeals Commission, or SIAC, cases, which concerned terrorism and people who were alleged to be terrorists, so I have some acquaintance with that part of the job. Of course, I did criminal work, so I have some acquaintance with that area as well.

Q48 **Lord Butler of Brockwell:** May we take it from Lord Judge's and Sir Stanley's opening statements that you think it is a good idea that this Bill in future sets up a single Investigatory Powers Commissioner?

Lord Judge: I have no doubt about that. We also have to make all the three current bits of the system work in the same way. I personally think, although I have no experience of IOCCO or Sir Mark's work, that the authorisation process is one of the strengths of what we do. You have to have an authorising officer who persuades you that this is appropriate—i.e. necessary and proportionate.

Lord Butler of Brockwell: If I may then clarify my understanding of this, in your area, Lord Judge, there is pre-event judicial authorisation.

Lord Judge: Of every item of intrusion that comes within our jurisdiction for prior approval by a Surveillance Commissioner.

Lord Butler of Brockwell: In Sir Stanley's area, this Bill will set up, except in the most urgent cases, pre-event judicial authorisation. Is that correct?

Jo Cavan: It will in relation to interception warrants, but it will not in relation to acquisition and disclosure of communications data, which is the bulk of our remit. Around 500,000 requests for communications data are made on an annual basis, by a rather large number

of public authorities. The judicial authorisation and the double lock that the Bill introduces are only in relation to the interception warrants, of which there are around 2,700 a year.

Lord Butler of Brockwell: Thank you very much. Then, if I understood what Sir Mark said, in the case, however, of somebody placing a bug in premises, there will be no judicial pre-event authorisation. There will be a warrant, but there will not be a judicial pre-event authorisation.

Lord Judge: If it is an application under part 3 of The Police Act 1997, which we deal with a lot, there will have been a pre-judicial authorisation in advance (for activity in a private vehicle or premises). This is why the system desperately needs to be shaken up.

Lord Butler of Brockwell: What about in the case of the intelligence agencies? Did I misunderstand Sir Mark?

Lord Judge: No, you did not. The intelligence agencies work differently. If it is an ordinary police investigation, yes, every piece of intrusive surveillance is pre-authorised. In the case of intelligence, it works differently.

Lord Butler of Brockwell: In the case of an intelligence agency, at the moment and under the Bill as proposed, there is no pre-event judicial authorisation of the warrant.

Lord Judge: No.

Q49 **Suella Fernandes:** What do you think about the safeguards provided in the new system as compared to the current one? Do you consider that there are better safeguards under the proposed system?

Lord Judge: I think that pre-authorisation is something Parliament needs to look at across the board—but I would, wouldn't I, because I am convinced about our own little bit? If you do that, the papers come through to a commissioner, who knows what the law is, knows what he—or she, but we do not actually have any females—is looking for. If it is not good enough, if it is an urgent or relatively urgent thing, he speaks to the authorising officer, saying, "This is not good enough. Tell me more about this" or, "I am worried about the possibility that this suspect's wife is going to have her life intruded on". If satisfied—and usually you are, because they do not come unless they have a good case—then it is authorised. Then you inspect at the other end and you go through them.

I will add this, which I did not mention when I made my opening statement. From time to time, my inspectors will tell me that they are very worried about the commissioner having given an authorisation. They are not just examining the way the police are doing their work; they are a form of check that the commissioners are applying the law. Of course, it does not happen very often, but that is part of the process and I welcome it. If there is a case where I think the commissioner was wrong to make the authorisation, then I see him and say, "I think this was wrong" or whatever.

Provided that you, as the citizen, are satisfied that, before people can come intruding in your life, a decision has been made by somebody independent of those who are going to do the intrusion, and there is a system for inspecting afterwards, at random, what the various bodies have been doing, that is a pretty good form of safeguard. In my experience—

again limited—I do not see cases where people or authorities are applying unless they have good grounds for doing so, because they know they will be refused.

Q50 **Lord Strasburger:** My questions are for Ms Cavan. I would like to start by congratulating you on the transparency of your reports and your engagement with the public through Twitter. I wonder if Mr McDonald's concerns about systemic difficulties and unwarranted activities would be allayed by the new commissioner being able to initiate inquiries on his or her own initiative, and perhaps even unannounced inspections. That is my first question.

Jo Cavan: On that note, we recently published a wish-list of some of the ways we feel the oversight provisions need to be strengthened. In one respect, the ability and mandate of the new commission to launch inquiries or investigations, we feel, could be further strengthened. We also feel that access to technical systems could be more explicit in the clauses. At the moment, the drafting is outdated: it refers to providing the commissioner with information or documents, whereas these days we are generally not looking at paper. When our inspectors go in, they have full access to the technical systems; they run query-based searches and look for compliance issues at scale, which is really important when you are dealing with these bulk collections. We think the oversight provisions and the clauses concerning technical system access and the ability to launch inquiries and investigations could be strengthened further.

Lord Strasburger: Lord Chair, would it be appropriate to invite Ms Cavan to put her views on how that might be strengthened to us in writing?

The Chairman: I am sure that would be fine.

Lord Strasburger: My second question is: how do you think we should strengthen oversight of international co-operation between Five Eyes intelligence agencies?

Jo Cavan: There are some additional safeguards in the IP Bill for the sharing of intelligence with overseas agencies. These matters have been significantly debated during some of the recent Investigatory Powers Tribunal cases. As a result of further disclosures made in those cases by the Government, the safeguards have been published and they are now in an amended code of practice. Certainly, that is an area we are looking at during our inspections and audits.

Sir Stanley Burnton: The fact we can interrogate the computer records of the authority whose activities we are auditing reduces the need for unannounced visits, because we have access to the raw data.

Q51 **Victoria Atkins:** Following on from Lord Judge's very helpful analysis of the oversight and review process, there is one angle that I am not sure the Committee has heard about yet, which is what happens at trial. Where an investigation results in a suspect being charged and a prosecution being brought, could you help us, please, with the duties on the prosecuting lawyer and prosecuting counsel to ensure that any warrants that may have been used during the course of that investigation were conducted properly, and the professional obligations on them as a reviewing process, in addition to all the reviewing processes you have already described?

Lord Judge: When everything has worked as it should have, and there has been no breach and no subsequent concern, that simply goes through. There is no disclosure. But, where there has been any breach—and, as Sir Mark pointed out, there are self-reporting breaches as well as discovered breaches—it comes to me, and it is axiomatic that the first thing I do, having decided what should happen about the breach, is to say all the papers must now be retained and disclosed to the Crown Prosecution Service, in the event of a prosecution, for onward disclosure as seen fit. That is up to the prosecutor. That material, I am sure, would then go to counsel for the defence, who would then decide whether to make an application or not.

The other feature, which has been underlined by a recent decision in the Divisional Court called Chatwani, is that there is an obligation—it is obvious that there is, but the court has said so—on the person making the application to tell the whole truth. In other words, you set out the points you say are favourable to the application you are making and the authorisation you are seeking, but you also have to add the bits that do not fit. Chatwani was a case where what was going on was not properly disclosed and the Divisional Court said, "Quite obviously, you cannot work on the basis that the whole story is not told". Failure to tell the whole story would itself constitute a breach, which would then have this system fall into place: retain it, keep it, disclose it if there is a prosecution. Of course, often there is not a prosecution, which raises a different problem, but if there is that is how it is done.

Victoria Atkins: In addition to the many sets of eyes in your organisations, there is also, if a case comes to court, the extra review conducted by lawyers and counsel to ensure that processes have been applied properly.

Lord Judge: Yes.

Q52 **Baroness Browning:** You heard me ask Sir Mark about training. I wonder what training you feel might be necessary for the new judicial commissioners.

Lord Judge: Rather like Sir Mark, what you are doing is making a judgment. This is what, if you are a former judge, you have been doing for however many years you have been doing it. You have been making decisions like this day in, day out. The questions are very simple: is this necessary? Where is the evidence? Yes, on this evidence, it is necessary. Is this proportionate? I must bear this in mind and that in mind, and that in mind. On this evidence, that is proportionate. Hang on, there is a bit of this that might involve the suspect having had conversations with his, for the sake of argument, doctor. You have to be careful there. I mentioned earlier an intrusive surveillance into the family car that is being driven by the wife. Nobody suspects her of anything, so you cannot have that; it is not proportionate.

That is all you are doing. You are making a judicial judgment, which is what you have spent your whole career doing. I am not saying you are infallible, and I made the point a few minutes ago in relation to my commissioners: when they get it wrong, my inspectors will tell me. But you do not need special training for that. What happened to me is, in effect, I went and shadowed my predecessor. I went out on inspections to see what my inspectors did and how they went about it, and to see that they were doing the job the way I wanted

them to do it. I go out with my commissioners. We meet regularly and discuss the problems that are current. That is the training, and then you take over the job.

Baroness Browning: With the advance of technology and things moving on so quickly, particularly once this is in one collective body, could the choice of methodology in the application that comes before you be something you question—whether this route is going to be used or that route? Does that not require some technical knowledge on the part of the person making the decision?

Lord Judge: Not really, because, for necessity, that does not arise. You do not need to know whether the nature of the intrusion is a probe that is one inch long or six inches long; you need to know whether there is going to be a probe. Of course, I have overlooked this. I spent time, two days ago, sitting in the National Crime Agency, being lectured to about how some of the worst aspects of child pornography being transmitted around the world are dealt with. We do try to keep up with that.

But, no, you are making a judgment. In the new system, I have no doubt—and I disagree with Sir Mark here—that there should be one or two people with serious expertise in technology. I also think there should be a legal adviser. The law is extremely complex. RIPA is a dreadful piece of legislation. I say that with some strength of feeling, having had to try to understand it. Why do judges need a legal adviser? For that reason: to say it could be any one of 17 possible interpretations, rather than the five you thought you had. More importantly, in this system, from time to time you need advice. That is what I would like to happen, but then I envisage this as rather different from the bits and pieces you are seeing put together before you today.

Q53 **Lord Hart of Chilton:** You heard us discuss with Sir Mark the question of the judicial review principles that underlie the judge's oversight. I wondered if any of you would like to comment further on what he said. We were exploring whether it is right to call it a real double lock system. Are there any points you would make, further to the points made by Sir Mark?

Sir Stanley Burnton: Judicial review is not simply a question of looking at process. In the context we are discussing, the commissioner has to look at necessity and proportionality. The degree to which judicial review is imposed as a test and the stringency of the test depend very much on the context, the facts of the individual case and the consequences of the administrative or governmental decision in question. In the context we are discussing here, it is not unfair to describe the process as a double lock.

Lord Judge: That is rather my view. My only hesitation, which is a lawyerly one but not totally without some force, is in using the words "judicial review" as a description of the test that has to be applied by the judicial officer. Judicial review used to be Wednesbury unreasonable mad. We would call it Wednesbury unreasonable, meaning only an idiot could have reached this decision. Nowadays, judicial review is less stringent than that: "He is not an idiot, but it is a really stupid decision". That is not quite the same. "I am not sure many people would have reached this decision" is another test. We need to be slightly careful.

If you are talking about the Home Secretary, and I think you are, I have a separate point. There is a difference between national security warrants and ordinary criminal warrants.

What we do should be the system for ordinary criminal warrants: an authorisation in advance. That is a double lock. National security is rather different. The Home Secretary has the most amazing responsibilities in relation to that. Judges second-guessing is simply inappropriate. You have to have a stringent judicial review test. I am now coming back to what Sir Stanley said. You know you are dealing with national security; you know somebody might be planting a bomb. You are going to be very cautious about interfering and saying, "This man or woman, who is the Secretary of State, is daft". So I think the double lock system will work pretty well.

Sir Stanley Burnton: You can forget about Wednesbury unreasonableness in this context. Interestingly, proportionality and necessity are tests that we have imported from Europe, and the proponents of the Bill are clearly happy to adopt them in this context.

Q54 **Matt Warman:** As a still fairly new Member of Parliament, it struck me, observing the procedures of Parliament, that, if you have some pretty crazy procedures around for long enough, they become lauded as institutions. You described a pretty crazy set-up in your opening remarks, but does it not function as a sort of quadruple lock on what we have already, if you are constantly going back to ask for re-authorisation? I wonder what we are going to lose by streamlining it, if anything.

Lord Judge: I am sorry, I must have been unclear. They are not re-authorisations. Each one is a fresh authorisation by a different body. Sometimes the body will not even know what the earlier authorisation was. It is not a quadruple lock at all. Each is an individual one.

Matt Warman: So you do not see any strength from having three different people.

Lord Judge: No. I see potential for confusion. A much more coherent system would enable the same commissioner to look at one case. "This is the case of Snooks. This is the drugs ring. Right, the undercover officer has gone in. Here he wants this. Does the authorising officer think this is appropriate? Yes", and so on. The whole thing can be kept, in effect, under one person's eyes. It is much more proportionate. Sorry I was not clear enough. They are separate organisations.

Matt Warman: The argument that has been put is: at the moment, we have three commissioners, and, if one person makes a mistake, who is checking up? You would not accept any of that.

Lord Judge: People make mistakes, certainly, but we are all independent organisations. We talk; we discuss problems together, but we operate completely differently. It is not a system with the three sections of this keeping an eye on each other. We do not.

Q55 **Lord Butler of Brockwell:** When we took evidence from Home Office witnesses last week, they introduced a new concept, new to me anyway, of rationality. We asked whether reasonableness would be a test, and the witness seemed to dissent rather. He made a distinction between rationality and reasonableness. Is that a distinction you recognise?

Sir Stanley Burnton: The Wednesbury test is a rationality test: that no sensible administrator or executive correctly applying the law could have reached this decision. It is not a very stringent test; it is only in extreme cases that you are able to say something is Wednesbury unreasonable, whereas proportionality and necessity are more stringent.

Lord Butler of Brockwell: You are saying that there is no great distinction between reasonableness and rationality.

Sir Stanley Burnton: I am.

Lord Judge: I would not have noted any difference between them. I would not have argued the point with you. If you had said "Is it reasonable?", I would not have said, "It has to be rational".

Q56 **Stuart C McDonald:** I have a rather more mundane question about money, I am afraid. The impact assessment suggests that the new oversight and authorisation regime should cost around £150 million over 10 years. Would you regard that as realistic? If you do not feel able to answer that particular question, would you say that you have had sufficient resources to carry out your jobs fully, or are there other things you would have liked to do that you have been constrained in?

Lord Judge: I could give you a list of my complaints.

Stuart C McDonald: Please do.

Lord Judge: Our technology is, for obvious reasons, supposed to be secure. Our Brexit system—I am so sorry; I have something else on my mind—our BRENT system is hopeless, so we want it improved. We wait too long for new appointments to happen, and so on and so forth. Parliament has to decide how much it is going to spend on protecting the citizen from the threats of crime and terrorism, and how much it is going to spend on ensuring that those who should not be being surveyed in any way at all are protected from it. If you go down this route, you will have to have—I would strongly recommend if I were asked, so I will tell you anyway—a location separate from the Home Office, and people working there who are not drifting in and out of the Home Office. The perception of independence is strengthened by going to a separate place.

I mean no discourtesy; our rooms are pretty cramped. You are going to have a big system. If you have the same number of commissioners I have, which is six plus me plus three assistant commissioners, that is ten before you start. If Parliament enacts a system in which there is authorisation for everything in advance, it is going to take a lot more people. It will cost a lot more. We can either do it on the cheap or spend more money. We are in times of great financial stringency. I am sorry, but this is really not for me to say. I might say it in a different role, but not here. Yes, it will cost a lot more.

Sir Stanley Burnton: I am not an accountant and I cannot give you a figure. My impression is that in order properly to run the system, there are going to be something like eight judicial commissioners, which is quite a lot of staff. They must be backed up with appropriate staff, with the kind of skills my office now has but more widely available. There will be more inspectors, who must be appropriately qualified. You are looking at significant sums of money.

Incidentally, on a question that Sir Mark was asked, it ought to be the chief commissioner who determines what staffing and resources are needed. He must, of course, approach the Treasury and agree a budget, but it seems to me to be inappropriate for the person who is being monitored in a sense to be the person who decides on the resourcing of the office.

Indeed, internationally, one increasingly finds that judicial bodies are not subject to a Ministry of Justice, so far as resourcing is concerned. It is the judiciary that determines the resources it requires, subject to Treasury agreement.

Lord Judge: I entirely agree with that. The idea that judges will be looking at the Home Secretary's decisions and saying, "We do not think that is right", and then going cap in hand to that same Minister is not a sufficient separation.

Stuart C McDonald: That is helpful, thank you.

Q57 **Lord Henley:** I asked Sir Mark earlier about cost. This takes me on from Stuart's questions. Are you saying that under the new arrangements you should, almost as the universities used to in the past, negotiate directly with the Treasury without any intermediary?

Lord Judge: That would be my view. I make this clear: I am not seeking appointment to be the high panjandrum for this. A direct communication between the Treasury and the Commissioner is the way to do it.

Sir Stanley Burnton: As a matter of principle.

Lord Henley: Is that because your independence would be undermined if you had to go through the Secretary of State?

Sir Stanley Burnton: The appearance of independence is undermined if one has to go through the Minister whose work one is supervising.

Lord Henley: I ask that purely because I remember, back in the long, distant past, that that is how university funding used to be done when universities were independent. It is no longer the case; there is a department that looks after universities. That might be the way forward.

Lord Judge: In the context of the way the judiciary works, there has been coming and going about this, but I used to agree a budget or not agree a budget. I also had the power, which I never exercised, not only to write and say, "I do not agree it", but to say, "I am going public and this will not do". You need some kind of arrangement like that. We are both in the same place. If we are going to supervise the Home Secretary, we must not be answerable to him or her for the money.

Q58 **Lord Strasburger:** Would you be attracted to the system that exists in New Zealand, where the people in your position have a fixed percentage of the spend on intelligence and policing, and the decision is taken out of politicians' hands?

Lord Judge: The decision as to money?

Lord Strasburger: Yes.

Lord Judge: Ultimately, the Government have to find the money, so there has to be a discussion with somebody who represents the Government. Therefore, that is why we both say the Treasury.

Sir Stanley Burnton: I think I would need notice of that question.

Jo Cavan: If we went to that type of model, our percentage would no doubt be significantly lower than the percentage in New Zealand, because of the larger scale of our intelligence agencies, in particular the bulk collection we do, in comparison to New Zealand. Anyway, I do not necessarily think it is a bad model. I would say that the legal mandate and oversight provisions the New Zealand inspector general has are far more explicit and comprehensive than the ones in this Bill.

One of our points on the clauses around oversight is that they relate only to judicial commissioners; they do not relate to the commission. If we are going to create this world-leading oversight commission, it is important that the commission is explicitly referenced and the legal mandate, powers and functions are comprehensively covered.

Lord Strasburger: For the second time, I will say something about judicial review. I asked the Home Office on Monday why the words "judicial review" were in there, and they could not really tell us. What would be the effect, do you think, if they were struck out? Would the Bill be better for it, or worse?

Lord Judge: Parliament has to decide what function the judge is to exercise. Judicial review is a well-known series of principles, even though occasionally you hear it expressed in different ways. As I said a few minutes ago, in terms of national security, the idea of the judge in effect making the decision simply cannot arise. If a bomb goes off in London tonight, it will be the Home Secretary who will be down there. It will be she who has to answer to the House about what has gone on; it will not be the judge. We have to be careful to remember that there is a political responsibility, which is in the hands of the Minister, and we cannot dilute that.

Sir Stanley Burnton: If I remember rightly, the legislation on control orders, which are orders short of imprisonment to control people who are suspected to be terrorists, also requires the judge to apply a judicial review test. In practice, of course, in SIAC, the judge hears, often in secret, the evidence that is available to show that someone is a security threat. He applies quite a stringent test, because he has the information and knows whether there is something justifying imposing a control order. The legislation has changed, but it is not dissimilar.

Q59 **Bishop of Chester:** The fear in some quarters is that this new system will end up with rubber-stamping, that it will not be sufficiently independent. That is the fear abroad in some quarters. I am trying to imagine life in the increasing digital swirl in the years to come, with the exponential growth in communications and means of communication. How can we get some feeling of control and exercise oversight, and not simply be carried along in the tide? The threats in the 21st century will probably increase as well. Can you give us some idea as to how this double lock, this independent supervision, will work in practice?

Lord Judge: I hope I am not being discourteous. It is very easy to drum up anxieties. I am just as worried about criminals being able to get hold of information as I am about any of the authorities. We concentrate on the authorities. I do not know what is going on in this room even as we speak, but the technology available to serious criminals is, at the very least, as good as is available to law enforcement people. You trust your judiciary to make decisions against the state when it is appropriate to do so. I do not think anybody suggests that the judiciary nowadays is less independent than it was. In many ways, it is more so.

You have men and women who have exercised these functions all their professional lives, first at the bar or as solicitors, then as judges. They are men and women of proven experience and quality. You just have to work on the basis that you should trust them.

Bishop of Chester: Would it be better for perception, if nothing else, if the appointment of the commissioners was not made by the Executive. Just as you made those comments earlier about having clear blue water between the Home Office and this, would it be better to involve an agency more independent than the Executive?

Lord Judge: It is the Prime Minister's appointment. The Queen appoints the Lord Chief Justice, but that is on the recommendation of the Prime Minister. I do not suppose the Prime Minister spends a lot of time deciding what he is going to recommend to Her Majesty. There is, in the case of the judges, a Judicial Appointments Commission. I would not recommend that for these appointments. Apart from anything else, they have far too much to do and it takes a very long time.

For the very last commissioner who was appointed to my team—and this you could consider—a senior serving judge and a member of the Judicial Appointments Commission sat together, with my predecessor as an observer, and they chose whom it should be, and the appointment was then made. That is a perfectly sensible system. It is only theoretical that the Prime Minister has anything to do with it. It is very nice for me to be appointed by the Prime Minister, but I honestly do not suppose anything more.

Sir Stanley Burnton: By prescription, the commissioners are going to be either actual serving judges or former judges, and so one has to bear in mind that they will have been independently appointed, initially. Whether they will be full-time judges working part time as commissioners or are expected to be full-time High Court judges seconded to the commission, the Bill does not make clear. We probably both have concerns about the ability of the existing High Court to have people seconded to a different function, given that the High Court itself is under pressure.

Jo Cavan: Before we move on, I wanted to talk about the end-to-end process, because a lot of the debate has been focused purely on the double lock and the authorisation process in the first instance. Yes, that is crucial, but what is equally crucial is the post-facto audit functions, which look at the process from end to end. We carry out over 200 inspections a year and make over 800 recommendations to improve systems and procedures in compliance.

The inspectors, during their inspections, are looking at post-authorisation: was the actual intrusion foreseen at the time the warrant or authorisation was given?; has the conduct become disproportionate because the level of intrusion was not anticipated? They are looking at how the material that has been gathered has been used. Has it been used in accordance with the purpose that was set out in the warrant? They are looking at the retention, storage and destruction procedures for that material. They are looking at whether any errors or breaches occurred as a result of the conduct. All those post-authorisation functions are critical to ensure that you are overseeing and auditing the end-to-end process. That is where the modification and ongoing review of these provisions come in.

Sir Stanley Burnton: The reviewer will also look at the duration of the warrant and may go to the public authority concerned and say, "How is it that this warrant has been renewed twice? What evidence have you been gaining from it? Was there any justification for its continuation for such a long period?'

Q60 Mr David Hanson: In relation to Clause 176, which establishes the budget, as we have discussed previously, are you therefore suggesting to the Committee that we should consider recommending a rewrite of that clause that separates completely the funding from the Secretary of State, not just in terms of the effective micromanagement that the clause could imply, although in practice it probably will not, but in terms of the principle that the Treasury should be the lead department that you directly negotiate with?

Lord Judge: If we retain the present Bill in relation to judicial oversight of the Home Secretary, yes, unequivocally.

Mr David Hanson: I have a second point. Lord Judge, I noticed you made the point that it is very nice to be appointed by the Prime Minister, but you are sure he does not take much interest in it. I suspect, as many people in the past, should you be a troublesome priest, he may take some interest in your reappointment. I am wondering, given what the Lord Bishop has said, whether or not consideration should be given to independent appointment, rather than direct ministerial appointment, into the oversight role, given that oversight role?

Lord Judge: If we envisage that, 20 years from now, the Prime Minister of the day decided that he or she was not going to re-appoint somebody, and had no good grounds for doing so save that he or she did not like the colour of their face, or whatever it might be, there would be an absolute scandal. I really do not think Prime Ministers would want to get embroiled in that sort of thing.

We have to be careful about public perception, if you do not mind me saying so. Most members of the public, I suspect, want to know that those of us who have responsibilities in this field are seeing that the job is done efficiently, ie to protect them, and fairly, to protect their own rights. That is what they want. I do not think that they are going to be terribly fussed, largely, about whether the Prime Minister's name goes on the appointment, or whether it is that of the Speaker of the House of Commons or the Lord Speaker. One has to be careful. That is my view about it. If I were in charge and, the Prime Minister failed to re-appoint somebody and I thought this was the reason, I would go and see the Prime Minister and tell him, "I will go public about this".

The Chairman: Thank you very much indeed. It was a fascinating session and we are grateful to all of you for coming along. You have given us very interesting stuff to chew over, to say the very least. Thank you very much indeed.

Lord Judge: Thank you.

Martin Chamberlain QC (QQ 186-196)

Evidence heard in public Questions 186-196

Oral Evidence

Taken before the Joint Committee

on Wednesday 16 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Lord Butler of Brockwell, Bishop of Chester, Lord Strasburger.

Witness: **Martin Chamberlain QC**, gave evidence.

Q186 **The Chairman:** A very good evening to you. I am sorry that we are a little later than we thought, but we have had a couple of fascinating sessions. I have not the slightest doubt that this will be equally fascinating. You are all most welcome to the Committee. As you know, in these situations different Members of the Committee will ask different questions, but I am going to ask a very general one, which perhaps gives you an opportunity to make a general comment on the Bill that the Committee is considering, if you wish to. Aside from the new powers on the retention of internet connection records, in your view, does the draft Bill consolidate existing powers or extend them? In answering me, if you wish to make any more general comments, please do so.

Matthew Ryder: The answer to that question depends slightly on, when you talk about extending the powers, whether you mean extending what the security services and the authorities are already doing and what they say is authorised, or what others would say is currently authorised under the existing legislation. There is a dispute and lots of litigation about what is or is not currently authorised under the existing legislation.

My view would be that there are a large number of new powers that are not properly authorised within existing legislation. Just to go through them with headlines, in Part 1 of the Bill, thematic warrants are allowed in relation to Clause 13. There is not a thematic warrant provision for targeted surveillance and targeted interception within RIPA. I know that the Government say that, if you cross-reference Section 8(1) with Section 81, you can find group surveillance as part of targeting but, realistically, thematic warrants are something new, and the idea that you could target people as groups by their activity is something new in part 1 of the Bill. It is important because, conceptually, it is anathema to the existing culture of surveillance that has been going since the 18th century in this country. If we are to move in that direction, it needs an informed parliamentary debate about it, to decide if we want to go in that direction.

Secondly, mass surveillance or bulk interception—whatever you want to call it—under Part 2 of the Bill is essentially something new. I understand—I was involved in the case and litigated the case in the IPT last year—that the Government say that bulk interception or

bulk collection is permitted under Section 8(4), but there is a dispute about that. There is a case on its way to Strasbourg. It has been communicated in Strasbourg. There are many of us who would say that it was not set out very clearly, if it was permitted at all, in RIPA.

Part 5, on equipment interference, is really new. It has really emerged only since the draft code of practice was published in February 2015 in response to ongoing litigation. It turns out that the Government's position on the existing power is that it is a very broad power, under Section 5 of the Intelligence Services Act, combined with the draft code that they published on the door of the court in February 2015, so equipment interference is new. It is a very significant power that requires a lot of scrutiny and debate.

Part 7, on bulk data sets, is essentially new, has not been regulated before and is not in the existing legislation in any meaningful way. The power to have access to bulk data sets and how they would be defined is something new.

I missed Chapter 2 of Part 6 on bulk communications data acquisition. That is essentially new. In other words, the large collection of communications data in bulk is something that was not clear from any legislation before. That is essentially being regulated for the first time, under this Bill.

Finally, it is arguable—this is more debateable—that Clause 189, which is the clause that has tech companies particularly concerned, is if not new then certainly of new significance, because it requires telecommunications service providers to maintain their capabilities and combines that maintenance requirement that existed in RIPA with a new definition of a telecommunications service and those who are providing that service. It is broadened out by Clause 193(12) to those who are allowing those communications. That means that those companies that simply have communications apps that facilitate communications through the internet, such as Facebook, Apple or those sorts of companies, may be caught in a way of maintaining their capability that they had not imagined before. That opens up the question of whether encryption is engaged in relation to that issue and, if it is not in the Bill as it stands, in due course whether that is a concern. In summary, there is quite a lot here that is very new and these powers are important. They are significant and, therefore, because they are new, they would require debate.

Martin Chamberlain: That was a very comprehensive answer that enables me to be much briefer. The answer to whether and to what extent the Bill contains new powers is very difficult, for this reason. In the run-up to the tabling of the Bill a number of things that nobody knew the agencies were doing, they were revealed to be doing under the existing powers. There has not been time for some of the things that we have very recently found out the agencies are doing to be tested in legal proceedings. I am thinking there particularly about the use of the extended definition in Section 80 of RIPA effectively to enable thematic warrants to be issued, and the use of Section 94 of the Telecommunications Act 1984, which is something we found out about for the first time in the immediate run-up to the tabling of this Bill. As to whether those activities that we now know have been undertaken by the agencies are lawful under RIPA, the answer is that it has not been tested and so it is very difficult to know.

Generally speaking, whether the Bill confers new powers is, with respect, not a terribly helpful question. One of the important purposes of this Bill is to get a democratic mandate

for things that have not yet had a democratic mandate. Whatever you might say is the correct judicial interpretation of some of the old powers, certainly it can be said, without any doubt, that quite a lot of the things in this Bill are things that nobody in these Houses of Parliament has examined the justification for, to date. Are they new powers? One can debate that. The courts have not had the opportunity to debate it, in many instances. They certainly are new in the sense that they have not had a democratic mandate, in many cases.

Peter Carter: Needless to say, I agree with all that has been said, so I shall be even shorter, I think. This Bill is important, because it enables the democratic process to take control of what has hitherto, to a large extent, been a hidden exercise of what is known as a prerogative. It is about time that the prerogative powers were brought to heel and this is a good way of doing it.

Insofar as this Bill brings within the ambit of the law practices that hitherto have either been questionable or possibly outside the law, there is a huge amount to commend it. Only if the kind of activities that this Bill encompasses are subject to law and lawful control, and therefore lawful monitoring, can it be said that these powers are being exercised in a truly democratic way. We need the powers in this Bill, to some extent or another, to combat serious crime, terrorism and actions against the state. The exact extent is a matter for political debate, as well as legal debate.

One of the problems and one of the ways in which the current drafting of the Bill, potentially and exponentially, will extend the powers is in the definitions clause, Clause 195, which includes a definition of data. As Matthew has said, one of the things that appears to be an extended power is the bulk acquisition of data. Data is defined in Clause 195 as including any information that is not data. Therein lies a problem.

Graham Smith: I am going to be slightly longer. I have identified quite a few new aspects that are potentially new powers in this. First, although the question caveats out internet connection records, we do need to understand that, when one looks at Clause 71, which is the power to issue data retention notices, and one compares it with the existing data retention powers in DRIPA, as amended by the Counter-Terrorism and Security Act of 2015, and if one adds internet connection records to that, Clause 71 still goes far beyond adding internet connection records to the existing data retention powers.

Although this has been presented as something to enable the retention of internet connection records, it goes far beyond that in five or six different ways. Perhaps most significantly, the existing DRIPA powers are restricted to a few types of human-to-human communication—internet email, internet access and internet telephony. This would catch all the background activities on my smartphone that happen when it is sitting by my bedside when I am asleep, when I am away from it, whether it is receiving notifications, getting software updates or anything of that sort. It would capture and cover any machine-to-machine communication, which if you look forward to the internet of things would cover my connected home thermostat or my car checking if it needs a software update. Essentially, anything connected to the internet or indeed any other type of network would fall within Clause 71. It now applies to private services and systems, as well as public, and of course the power to require data to be generated for retention, not just retained, is completely new. The previous limitation to retaining data generated or processed within

the UK has been removed, so Clause 71 is very much broader than one might think by just referring to internet connection records.

Other new and extended powers are technical capability notices, under Clause 189. At the moment, under RIPA Section 12, capability notices can be given to support interception warrants and nothing else. Section 189 will apply also to all the new types of thematic, targeted and bulk warrants, under Parts 5 and 6, and will also apply to support the acquisition of communications data under Part 3. All of that is new.

In bulk interception, there is a new power. I call it a new power, but it comes as a result of the warrantry definitions; however, there is effectively a new power to extract related communications data from content and to treat it as related communications data. For instance, if I send you an email saying, "Here is somebody's email address", that is part of the content of my email, but the email address can be extracted from the content and then treated as related communications data. That is very significant, because most of the restrictions on examination of content do not apply to related communications data, so it is very significant. That is replicated as well in the new bulk acquisition and equipment interference powers, which talk about equipment data, which is more or less equivalent to related communications data. There is the power to extract equipment data from the content that is acquired in that way.

Lastly, there is the extension generally through the knock-on effects of the expansion of the definition of telecommunications operators in the draft Bill.

The Chairman: Thank you so much. They were some very useful answers.

Q187 Matt Warman: Given that we cannot agree on what is meant by new, I slightly hesitate to ask this. The Committee has been blessed with lots of different interpretations of what judicial review will mean in the context of this Bill. What do you think judicial review terms would mean, as far as the authorisation of warrants would go, in this new Bill?

Martin Chamberlain: You have just heard from David Davis about Lord Pannick's article in the *Times*, where he suggested that, in this kind of context, the judges would be applying a high intensity of review. One can explain it in this way: whenever a judge is applying a judicial review standard, there is a spectrum of different types of intensity of review. At one end of the spectrum, there is very light-touch review, which David Davis accurately described as, "Don't touch it unless it's totally barmy". Then at the other end of the spectrum, there is a real rolling up of the sleeves, getting into the detailed kind of review, where the judge comes close to substituting his or her own judgment for that of the ministerial decision-maker.

Practically any judicial review practitioner will tell you that, in practically any judicial review case, a key point of contention between the parties is where on the spectrum that case lies. Is it a light-touch case, is it an intensive-review case or is it somewhere in between? David Pannick's article in the *Times* suggests that this would be an intensive review kind of case. David Pannick is generally right about most things, but I would venture to suggest that you need to apply a bit of caution to whether that is correct in this context. Certainly it is true that a warrant authorising interception involves an invasion of someone's privacy,

but it does not involve the kind of restriction of liberty that you see in, for example, a control order case or a TPIM.

The Committee suspended for a Division in the House.

Matt Warman: You were in full flow on what judicial review is likely to look like in this context.

Martin Chamberlain: I have explained that there is a spectrum in judicial review, in terms of intensity of review, with very light-touch review at one end and high-intensity review at the other. David Pannick thinks that, because of the privacy context, we would be in the high-intensity part of the spectrum. I question really whether that is correct. The reason I question it is this: the matters under review, under Clause 19, are whether the warrant is necessary and whether the conduct authorised is proportionate. If you just concentrate on that second question, you are asking yourself the question as a judge reviewing this warrant whether the national security benefit to be derived from the warrant is proportionate to the intrusion into privacy that it involves. That is, to my mind, typically the kind of question on which judges will give a great deal of what used to be called deference—some of the later judgments deprecate that term, but leeway or latitude, however you want to put it—to the elected Minister. That is what would normally happen in judicial review. There is a House of Lords case called *Rahman* that makes that point. Where you are looking at proportionality assessments by a Minister who is accountable to Parliament, you apply a very light-touch review.

The touchstone, if you really wanted to get an interesting answer to this question of where on the spectrum it lies, is to ask someone from the Government what they think and see if they would be willing to give the kind of parliamentary statement that could be relied on in subsequent legal proceedings, to say that what they meant by judicial review was intensive review. I doubt whether you would get them to say that, because I suspect they would want to reserve the position to argue in front of the commissioners that it was a light-touch review that was intended.

Peter Carter: I hope Lord Pannick is correct, but I also fear that it is so uncertain that he may not be. This is not an area in which uncertainty can possibly be allowed to be sustained. One of the problems about judicial review is a problem that was created by Lord Judge last year because, in a decision called *Regina v L*, a decision in the Court of the Appeal in which he gave the judgment, L was somebody who as a young woman who had been trafficked for exploitation. The question was whether it was right that she should be prosecuted for an offence that she committed as a result of her exploitation, which we would now call modern slavery. The issue was what test is to be applied to the decision of the Crown Prosecution Service to proceed with her prosecution, even though all the circumstances demonstrated that she was a victim of exploitation. The test to be applied is one of judicial review.

There was the kind of discussion that we have heard about: on the one side this; on the one side that. Lord Judge said that we are going to apply in this case a test that is not the conventional judicial review; it is something different from that. The difficulty was that he did not say what it was. I do not know anybody at the Bar, who practises in that area of

law, who understands what the test with which we are left in that area of law is. What I suggest is that the simplest way of removing this ambiguity is to suggest an amendment that you simply delete the words about judicial review.

May I go back to the stage about how the judicial commissioners will consider this? It starts off with reviewing what? A decision by the Secretary of State. Normal judicial review is a review of a decision and the reasons for that decision. Are those reasons irrational or are they rational? Do they include considerations that are immaterial or are they centred on considerations that are central to the issue in point? I do not think there is any provision in this Bill for the Secretary of State to give reasons for his or her decision. The judicial commissioner will not be reviewing reasoned decision. The judicial commissioner will be reviewing the decision and, therefore, ought to be reconsidering from scratch whether or not it is appropriate to authorise this warrant and doing so by applying the test of necessity and proportionality.

There is one slight twist about this because, by Clause 169(5) of the Bill, "In exercising functions under this Act, a Judicial Commissioner must not act in a way which is contrary to the public interest or prejudicial to … (a) national security, (b) the prevention or detection of serious crime, or (c) the economic well-being of the United Kingdom". I cannot imagine for a moment that any judge or judicial commissioner would act in a way that is contrary to the public interest, but who is to determine and who is to assist the judicial commissioner on what is national security, what is in the economic wellbeing of the United Kingdom, particularly if the judicial commissioner is not assisted by reasoning from the Secretary of State? If there is to be reasoning from the Secretary of State, how long is this process to take and why not simply remove the Secretary of State from the process?

Matthew Ryder: May I just make two very short points on this? The first one is that the role of the judge in judicial review, when it has been explained, might be slightly confusing in the sense that there is talk about deference. The question might be what the judge would add in making a decision, if he is going to be so deferential. That is to do with the role the judge has in judicial review, versus the role that the judge would have if the judge was having to authorise it themselves.

I have drawn an analogy here, because it goes back to some of the discussion we overheard from the previous session. There are times when this conversation seems as though it is discussing the difference between political accountability and judicial accountability. One has to remember that the authorisation, in this process, is one very small part of an overall operation, the vast bulk of which is not decided by the Home Secretary or a politician, but is decided by police and judges.

For example, Schedule 5 to the Terrorism Act which is the part that controls terrorist investigations, contains a large number of provisions, production orders and search warrants, including producing material from journalists, all of which are decided by a judge. Those can be much more intrusive, in some circumstances, and much more serious than intercepts, but we trust that to the judge. In serious crime operations, we trust search warrants and production orders to a judge, for a judge to make that decision. The judge does that not by deference to a ministerial decision but by having their own role in terms of making that decision for themselves, and it is a system that works very well with serious crime and under Schedule 5 of the Terrorism Act. That is why one can be led down a

cul-de-sac in thinking that we are choosing here between a brand new type of judicial authorisation or judicial role, when previously it had always been the Home Secretary. In reality in terrorist investigations and in serious crime, it is judges and police who are having to make those decisions and who are accountable for those decisions—sometimes life and death decisions.

Q188 Victoria Atkins: I should declare that Peter Carter and I were in chambers together. Mr Carter, you have talked about there not being any provision in the Bill that you can identify for the Secretary of State to give reasons. I have to say, listening to that, I thought, "Crikey, this is a lawyer's paradise". Is it not? We heard from Mr Davis earlier. He estimated that there are 2,300 intercept warrants a year that the Home Secretary does, which equates to nine a day, in addition to all their other duties. If the Home Secretary is having to sit down and write out reasons, in the way that you and I understand as lawyers, I fear that would be a real burden, adding bureaucracy in what is a highly dynamic environment. Is it not better to look at the evidence from the security services or whoever is making the application? Look at that and then the judge looks at it again—the same evidence—and makes their decision according to the evidence placed in front of them by the security services.

Peter Carter: I entirely agree. We do not want this to be a lawyers' paradise. It is going to defeat, not assist, the end. If the law is clear, there is less room for lawyers to get involved. You do not want lawyers getting involved to try to disentangle what ought to be a clear and transparent process for those who need to know about it. My only slight difference of opinion with what you suggested is I do wonder whether the Secretary of State needs to be involved at all, other than in those things that involve the security services.

Q189 Suella Fernandes: I have a question; I think Peter and Martin dealt with judicial review. We have heard evidence from Lord Judge and Sir Stanley Burnton, who have stated that they think it does strike the right balance, but proportionality involves a balancing exercise—a consideration of the objective and whether the objective is sufficiently important to justify the intrusion, whether the measures are directly related to the objective and ensuring that it goes no further than what is necessary. Do you not think that that encompasses a very clear and balanced assessment of the decision to issue a warrant?

Peter Carter: I do and those words are perfect, provided they are left alone.

Martin Chamberlain: I have to say that I am not quite so sanguine that the word "proportionality" necessarily connotes a high-intensity review. Within the case law on proportionality, under the Human Rights Act for example, there is still a very broad spectrum of intensity of review and, sometimes, even though the court is looking at proportionality, it gives the decision-maker considerable latitude. In other contexts, it gives the decision-maker rather less latitude.

The problem with simply saying that the standard to be applied is judicial review is that we do not know what arguments the Government will make to the judicial commissioners, and it is quite possible that the Government will say that this is the context, balancing the needs of national security against the intrusion into privacy, where you have to accord considerable latitude and discretion to the elected Minister, and where the judge really should not interfere, unless the Minister has obviously struck the wrong balance.

Suella Fernandes: Just by way of follow-up, would you confirm for the record that, in the process of judicial review, a judge would have access to the same information that was before the Minister throughout the original decision-making process? Is that your understanding of judicial review?

Peter Carter: Victoria Atkins made the point that this is a dynamic process and I entirely agree it is. Given the reality of the situation, particularly if it is a security service application for a warrant, it may well be that, by the time it gets to the reviewing judicial commissioner, which may be 15 minutes or half an hour after the Secretary of State has made a decision, further information is available. The judicial commissioner must take account of all the information that is then available, just in case there has been a shift—either augmented information or something that turns out to need correcting.

Q190 Lord Butler of Brockwell: When Mr Carter read out Section 169(5), saying, "In exercising functions under this Act, a Judicial Commissioner must not act in a way which is contrary to the public interest or prejudicial to—(a) national security, (b) the prevention or detection of serious crime, or (c) the economic well-being of the United Kingdom", I thought to myself, "Crumbs, that really is going to shackle the judge". It is certainly putting pressure on him to approve the warrant, but then I looked down and Section 7 says that that subsection does not apply "in relation to the functions of a Judicial Commissioner of—(a) deciding whether to approve the issue, modification or renewal of a warrant or authorisation". Perhaps you did not intend to mean that it was going to shackle the commissioner.

Peter Carter: No, I do not think it is. What I was concerned about was any suggestion, as perhaps had been made by one of the previous witnesses, that judges were going to be bowled over by a suggestion that this is for national security and, therefore, you must not intervene. The point is that the fact it is there will not prevent the judges from having a rigorous and robust appraisal of the information that is before them, before they make an authorisation or not.

Lord Butler of Brockwell: You are saying that this does not shackle the judge. It will enable the judge to reach full discretion.

Peter Carter: I think so. I hope that the reference to "contrary to the public interest", in any circumstances, would not be something that a judge would find difficult to understand.

Matthew Ryder: I was just going to say, in relation to the point you are making and the point made by Ms Fernandes, it is important to bear in mind that a judge in this position may have access to material, but a judge is not making his own assessment of the facts in judicial review. In the situation where a judge is assessing a search warrant or a production order in relation to something very sensitive, like Schedule 1 to PACE, which could be obtaining material from a journalist, or Schedule 5 to the Terrorism Act, which could be very sensitive and very serious, a judge has the evidence but then assesses that evidence. If the judge thinks the evidence is not sufficient, he could call for more or could look at it.

In a judicial review situation, the judge is essentially bound by decisions and assessments of facts that have been made by the Secretary of State and is applying judicial review principles—which, as Martin rightly says, can be on a range of scrutiny—to that assessment that has already been made of the facts.

The final point to bear in mind is that, normally in judicial review, there is an element of an adversarial process. In other words, the judge is assessing it with somebody making representations in relation to the other side. There will be no adversarial process built into this, the way it stands at the moment. You will have a judicial review, but no one putting forward the argument to the judge in a different situation. Now, that is not unheard of; you have that in other situations, but not in relation to a judicial review situation. That is why it is so important, in this sort of situation, for the judge to be able to be hands-on to potentially look at the facts and evidence in front of the judge, for themselves, and make that decision not shackled by any previous assessment that has been made by the Secretary of State.

Suella Fernandes: Do you not think that that will have a negative effect on timeliness and the speed of decisions, in urgent situations when there are real risks, in terms of the quality of decision-making?

Matthew Ryder: It should not do at all. The reason is that it does not have any problem with timeliness in relation to Schedule 1 of PACE. Those can be extremely urgent applications for very sensitive material in the most intense operations. It does not have any problems in relation to Schedule 5 of the Terrorism Act. I could not imagine a more serious situation, where a judge is having to decide on production orders or search orders in relation to terrorism investigations, under Section 39 of the Terrorism Act 2000, which are then being dealt under Schedule 5 of the Act.

Q191 Lord Strasburger: Not only am I not a politician, I am not a lawyer and I have been struggling through the fog of arguments in this area, since this Committee started to sit. It is only just now that I am beginning to see some light at the end of the tunnel. Are you collectively saying that the solution to this whole problem is to strike out the phrase that includes the words "judicial review"?

Peter Carter: Are you asking four lawyers to agree?

Lord Strasburger: I will settle for your individual opinion.

Peter Carter: My opinion is yes.

Martin Chamberlain: Mine is, too. It would be much clearer if you said to the judicial commissioners what standard you are expecting them to apply. You could do that in various ways. One way would be to get rid of the words "judicial review", which imply this shifting spectrum, without telling you where on the spectrum you are.

Matthew Ryder: I would still be inclined towards judicial authorisation by a judge, rather than judicial approval. I certainly think in relation to police cases that "judicial authorisation" would be appropriate. In national security cases, you can have a different discussion, but my preference would be "judicial authorisation", rather than "judicial approval".

Graham Smith: I am a mere IT and internet lawyer. I would not begin to venture an opinion on this.

Lord Strasburger: May I then ask the opposite question? What do those words add to the Bill? What benefit do they bring, if any?

Martin Chamberlain: The suspicion or the worry is that it may be argued by the Government, once this Bill becomes an Act, that what they add is a clear signal or flag to the judicial commissioner that, when you are examining warrants issued by an elected official, you should back off and not question those warrants, unless the decision to issue them was irrational or something close to irrational. Probably "irrational" is the wrong word, because clearly proportionality comes into it but, at the far end of the spectrum, that is the worry. It would be very interesting to hear what the Government say in response to that. If they were to say, very clearly, "That is not what we intend. We intend it to be intensive review", and if they were to say it in a way that could then be subsequently relied on in legal proceedings, that would be very interesting.

Q192 Dr Murrison: We have moved quite a long way towards the double lock. The double lock was a point of some controversy, but has now been accepted by the Government. It is worth just recording that. What you are saying is that you would be happy with the deletion of Clause 19(2), which we heard, for example from Liberty the other day, would materially improve the Bill and the scrutiny available.

May I press you on this five-day period, during which the judicial commissioner would take a view, albeit in the Bill at the moment a rather limited view, on the authorisation that the Secretary of State has given? Do you feel that five days is reasonable, since we have heard from others that it is a very long time for a judge to form a view, particularly since he is likely to be presented with the same sort of material that the Home Secretary deals with, sometimes with a very short timeframe? Indeed, that of course is used as a justification for the Home Secretary dealing with this in what have been characterised as emergency situations, not a judge. May I start? This is something that the Bar Council is particularly concerned about. We can see no justification for that five-day gap. The Secretary of State is a single person. Numerous judicial commissioners can be appointed and, no doubt, will be appointed under the Bill. High Court judges are used to dealing with applications of the utmost urgency.

When there is a need for an urgent application, for example a place of safety order or to prevent somebody being deported from the United Kingdom, I am afraid judges used to be wakened at any time of the day or night and can deal with that matter, as a matter of urgency. There is no reason why a judicial commissioner cannot deal with it as a matter of urgency. For example, a judicial commissioner might be in a position, as the Home Secretary probably might not, under the Bill, to say, "Yes, I authorise this warrant and I want you to come back in 24 hours and I will review my decision and how far it had got". There is provision for that in the Bill, but I can see that practice would develop whereby a judge would make an authorisation that was interim and conditional. I cannot see any reason why five days for a warrant that is potentially unlawful can be justified.

The Chairman: Can you suggest a time?

Peter Carter: I do not think there is any justification for any time, any delay. The delay, if anything, is going to be with the Home Secretary, not with the judicial commissioner.

The Chairman: The issue is one of urgency here, is it not? These are only urgent warrants. We are not talking about the 2,500 to 3,000 warrants that have to go through the various Secretaries of State. We talk about a much smaller number. Would that make a difference in terms of, I do not know, a day afterwards?

Peter Carter: The difficulty about that is that, if it is urgent, you should not prescribe a time limit because, if it is urgent, it must be done immediately.

The Chairman: Indeed, but the issue is if there is a joint authorisation, which there is on a normal warrant, but an urgent one, because of its very nature and what might be happening, the Secretary of State obviously has to authorise. The Bill says you can have up to five days for a judicial commissioner to review that, but you do not think there is any need for any sort of time limit. It depends on the availability of the judicial commissioner, presumably.

Peter Carter: There will be a judicial commissioner available at all times. There should be. It may well be that, if it really is urgent, the Home Secretary or the Secretary of State should be, as it were, a bystanding participant and it should be a single, consolidated process.

Matt Warman: How does that work?

Paul Hudson: The principal decision-maker and authoriser would be the judge. It would be subject to the Home Secretary saying, yes, he or she confirms that it is necessary, so you do it the other way round, in a sense.

The Chairman: To put in my own experience, from when I used to authorise warrants as a Secretary of State—very urgent ones, virtually in the middle of the night or something—you are not going to sit there and have to phone up a judge immediately, when something might have to be decided in minutes, surely.

Peter Carter: That is why I am suggesting that the only reason for having the Home Secretary's decision is this double lock process, is it not? The presumption is that the Home Secretary is a politician who is attuned to security needs and would be the first port of call but, in urgent cases, there is no need for that. The first and only port of call is the judge. If the Home Secretary, having been informed of the information says, "Actually, I disagree", which is highly unlikely, the Home Secretary would then have the power to revoke it.

The Chairman: Why are you suggesting that it should go to the judge before the Home Secretary in an urgent case?

Peter Carter: It is because you then have the consistency of every such warrant having judicial approval.

The Chairman: I understand.

Q193 Bishop of Chester: Is it possible to try to situate this whole discussion between the European culture, which has experienced totalitarian Governments and has a suspicion of government with the history of totalitarian interference, and North America, where there has always been that freedom of the individual and a small state. We are somewhere in between. There is a danger of these wide-ranging powers, which you have identified, being accepted

too easily, hence the need for some sort of robust double lock and a strong culture of judicial independence in the judicial element, I suggest. One of the questions we have raised is if the judges should be appointed by the Prime Minister or by the Judicial Appointments Commission. Should they be appointed for a single term of office, rather than have to submit to reappointment? There are these sorts of questions. Are there other ways of strengthening that culture of independence that you all want to see in the judicial involvement?

Peter Carter: Given the gravity of the kind of situation that is envisaged in this Bill, I would have thought that the appropriate candidates for judicial commissioners are likely to be High Court judges. It may be that it is because we have all gone native in the profession that we see no reason to doubt the integrity and the robustness of people who satisfy the criteria of appointment to the High Court bench. I do think, though, that there is a potential problem of perception, if not reality, if appointment to the judicial commission is by the Prime Minister, rather than by the Judicial Appointments Commission, with consultation with the Lord Chief Justice. That would be more appropriate, rather than it looking like a political appointment.

Bishop of Chester: Would you review after three years, as is proposed, or is it better and more of a culture of independence to appoint for a single longer term?

Peter Carter: I am not particularly bothered. Others may take a different view about that but, if you are appointing somebody of the category I have suggested, either they will be sitting senior judges, in which case after three years they may go back to their normal judicial appointment; or they may have retired, in which case three years would probably be sufficient for them to feel that they have done their job and would quite like to go and do something else. Potentially, it will be quite an onerous job. For somebody in this position, I do not see that there is a problem about the perception of independence from it being a three-year term, in the same way as, for example, for the appointment of the Director of Public Prosecutions, the term is sometimes three years and sometimes five years. Nobody, so far as I am aware, has made any suggestion of lack of independence as a result of a three-year, as opposed to a five-year, term of appointment.

Matthew Ryder: Three years is a short tenure for a judge and it might be that the Judicial Appointments Commission would be well placed to express a view about that sort of time in relation to judicial independence, because they have done some significant thinking on how long tenures should be for judges, to ensure that judges do not feel vulnerable when they next come up for review.

Bishop of Chester: When they appeared before us, the impression given by the judges was that they generally sided with the application. David Pannick's article referred to that benefit of the doubt or margin of discretion or whatever it was he said. I cannot remember the term you used there. One can see that a certain culture of it being normal to go along with the Executive could develop without quite being noticed. I simply put this up for you to demolish. Others who have sat in those seats would certainly have those anxieties.

Peter Carter: All you have to do perhaps is look at the history of the current Investigatory Powers Tribunal and the independence that has shown in standing up against the Government's attempts to keep secret the unlawfulness of some of the conduct, and the tribunal's insistence on making public as much of its judgments as it possibly can.

Martin Chamberlain: I would agree with that. I do not think you need to worry that the people who are appointed to these rules will slip into a culture of doing what the Executive want. What you need to worry about is that judges, in performing their role, will do what they think Parliament has told them to do. If they think Parliament has told them, by use of words like "judicial review", to accord considerable latitude to a constitutionally accountable Minister, then that is what they will do. That is not because they are unable to stand up to the Executive; it is because they are honestly interpreting what you have said to them. If you do not want them to apply considerable latitude, you need to make clear that they are not to do so. If you make that clear, they will do what you say.

Q194 Victoria Atkins: Lord Chairman, I am very conscious that I am about to venture into a subject in which you are an expert and I am not, but it is a simple question. Have you taken into account the political sensitivities of Northern Ireland and the way the judiciary is viewed by some, in different parts of that part of the country, when assessing the argument that judges should always come first?

Peter Carter: No.

Martin Chamberlain: I have not either, but I would have thought that, if and to the extent that there are elements of the community in Northern Ireland who have less confidence in the judiciary than perhaps people would have in England and Wales, or Scotland, then one would have thought that those same elements would have a similar lack of confidence or even a greater lack of confidence in members of the Executive.

Dr Murrison: I have a very quick supplementary to that. Do you think then that that is another argument in favour of the Judicial Appointments Commission appointing commissioners, rather than the Prime Minister? If the Prime Minister appoints the judicial commissioners in relation to Northern Ireland, one would also have to involve the First and Deputy First Ministers.

Peter Carter: I first heard that argument raised at a meeting in Portcullis House on the eighth of this month, and it struck me then that I wished I had thought about it before. It seems a very good suggestion.

Q195 Suella Fernandes: The Home Secretary will have the power to amend the functions of the judicial commissioners. How do you envisage that power being exercised and what kind of modification might be envisaged?

Matthew Ryder: I do not know is my answer.

Martin Chamberlain: I would say the same. It is very difficult to envisage how it might be exercised. In principle, it could be exercised to add to the functions or to take away from the functions. One potentially worrying use of the power would be if it could be used to alter the test that a judicial commissioner has to apply when considering or reviewing the issue of a warrant. I do not know whether it is intended to use the power or that the power might be used in that way, and it would be an interesting question to get the Government's view on.

Peter Carter: Can I make a suggestion? It seems to me that the power to modify the commissioner's role should be confined to those roles that are not central to the authorisation of warrants and the continuation or renewal of warrants.

The Committee suspended for a Division in the House.

Peter Carter: I am very grateful for that, because it has allowed me to find my place in the notes. The question was about the Home Secretary's power to modify the role of the judicial commissioner, which appears in Clause 177. In the clause as it stands, there are no constraints as to which role or part of the role the Home Secretary can amend. This means that, if you decide to remove the expression "judicial review", the Home Secretary could, by his or her power of amendment, depending on who it was at the time, put it straight back in again, which may not be entirely satisfactory.

This provision, Clause 177, appears in part 8 of the Bill. There are various provisions there that explain or provide particular functions for commissioners, including that the investigatory powers commissioner in Clause 169 must keep under review the exercise by public authorities of statutory functions, and so on. I can understand why that kind of role or function is suitable for amendment, as circumstances and the law change. What I would suggest is that Clause 177 should be amended by adding the words, in subsection (3), "This clause does not apply to any function of the judicial commissioner under parts 1 to 7 of this Act".

Q196 **Victoria Atkins:** I am conscious of the time. Mr Carter, you have written a very helpful paper, on behalf of the Bar Council, regarding legal professional privilege or LPP. Can you help us with any concerns about LPP and investigatory powers and, if there are concerns, how they can be addressed? How would you recommend they be addressed?

Peter Carter: We have concerns, because there is nothing in this Bill that protects legal professional privilege. Legal professional privilege is the privilege of a client to have private communication with a lawyer, to obtain legal advice or for advice and assistance in the course of litigation, whether active or potential. Communications between a lawyer and a client are not all protected by legal professional privilege, and we are not suggesting that all communications between a lawyer and a client should be protected or immune from investigatory powers. For example, the Proceeds of Crime Act makes it quite clear that communications between a lawyer and a client covered by legal professional privilege are immune, but a client asking a lawyer for advice on where the best place is to stash his stolen loot is not. If there was information that led the police or the security services to believe that that conversation was about to take place, then they would be fully entitled, and I would applaud them, for putting in place some of the provisions of this Bill to get evidence that that was taking place.

The difficulty is that, if legal professional privilege, properly so-called, is not recognised as a privilege that needs to be protected, it strikes at the heart of our judicial system, not just the criminal system, but the judicial system. It is the integrity of the judicial system that is one of the guarantors of our state as a democracy.

Imagine the situation if a client in a commercial action were to say to me or one of my colleagues, “I am about to engage on a contract and I need your advice as to the international effects of this. It is with a Russian company. It is very sensitive because I have competitors in other states. Can you assure me that all our communications will be confidential?”. Under this Bill, my answer would be, “No, I cannot”, because I simply do not know.

The difficulty is that the wording used in Clauses 5 and 65 says that, where a warrant authorises any of the investigatory powers under this Bill, then any action taken in accordance with that warrant is lawful for all purposes. If the warrant authorises the interception or the gathering of data information concerning communications between me and the client, it would be lawful, even though under international law, European law and our historic law, such communications have been immune, as a matter of public interest. The fact that these rights are ancient is neither here nor there; what matters is that they are current and they are important. They are important for the confidence of citizens in the administration of justice.

Interestingly, when David Anderson produced his report, *A Question of Trust*, in a fairly short passage, he described why legal professional privilege is important. He said, if it is apparent that there is no guarantee that legal professional privilege is protected, it will have what he called “a chilling effect” on the relationship between client and lawyers, and their confidence in the entirety of our judicial system.

The Government fight fiercely for its own legal professional privilege, particularly for example when it is engaged in international arbitration. The Belhaj judgment in the Investigatory Powers Tribunal said this, “There was no dispute between the parties”, that is between the state and Belhaj, “as to the importance of protecting and preserving the concept of legal and professional privilege”. Why, therefore, is that recognised importance not reflected in the Bill? It is in various other statutes, including in the Terrorism Act 2000 and in the Proceeds of Crime Act, as I have already identified, and in the Police and Criminal Evidence Act.

The problem is that there was one clause, in the Regulation of Investigatory Powers Act, Section 27, that used that expression, “lawful for all purposes”. The House of Lords by a majority decided that that empowered a warrant to enable the investigating services, police and intelligence services to intercept communications covered by legal professional privilege between a lawyer and a client. In fact, what was uncovered out of that was of precious little significance, but it was a chilling effect. It has had a chilling effect. Those of us who practise sometimes in criminal law realise that what you require is to build up the confidence of a client in order to give robust advice, sometimes advice that they do not want to hear, but they need to hear. If they cannot be confident that the communication is confidential and secret, they will simply say nothing. That does not help anybody or anything.

Why is it not there? It is said by the Home Office that it is all right; it will be in codes of practice. Interestingly, Schedule 6 contains the only reference to something akin to legal professional privilege, and it is in paragraph 4 of Schedule 6. It says, “A code of practice about the obtaining or holding of communications data by virtue of part 3”, so it is confined to the powers exercised under part 3, not under any other part, “must include … (b)

provision about particular considerations applicable to any data which relates to a member of a profession which routinely holds legally privileged information", which I assume means lawyers.

There are two things that follow from that. The first is that it recognises, as is evident from the proceedings in the Investigatory Powers Tribunal, that the security services have access to sufficient information to be able to filter those communications that are communications with lawyers, so they know which communications are likely to trigger access to data or communications, which are or the subject matter of which is covered by legal professional privilege. They can do that.

Why is it that the codes of practice under paragraph 4 of Schedule 6 are confined to this particular area under Part 3? The codes of practice or the draft new codes under the Regulation of Investigatory Powers Act also have a provision about legal professional privilege, which does not guarantee the immunity of legally privileged material from access by and disclosure to the agents of the state. It simply says it is a serious consideration, before authorisation is given, not only when it turns out that legally privileged material has been accessed inadvertently, as part of a more general and legitimate operation, but even when it has been specifically targeted.

Whether that will survive a challenge in the European Court of Justice or in Strasbourg, I have my doubts. I am not certain about it, but I have my doubts and I have my doubts because, in international and in regional human rights law, one of the critical basic rights is the right to independent advice or advice from an independent lawyer. Advice from an independent lawyer is going to be worthless if the client and the lawyer believe that everything said is going to be heard by or accessed by the state.

The state, in the cases that are dealt with in the Investigatory Powers Bill, will in most cases, the chances are, face some kind of litigation involving not necessarily the person whose communications are accessed, but somebody else. Eventually, the chances are, the litigation, whether it be criminal or civil, will indeed be between the person whose communications are accessed and the state. The state would not want to be at a disadvantage if another state in international arbitration had access to all its advice. There have been various expressions about the importance of this right over the centuries but, as I say, what matters is its significance now as a right in a democratic society, which is regarded as a guarantee of a democratic principle and a guarantee that citizens are not at a disadvantage in their dealings with the state.

The Chairman: I shall have to curtail things in a second. I am just asking whether your colleagues agree with what you have said on this or have any additional points.

Matthew Ryder: I do not have anything to add.

Martin Chamberlain: Neither do I.

The Chairman: There is no dissention, which is very good. I am going to close the session now. We have, however, a number of questions we would like to put, if that is okay, to all four of you, in writing. I am conscious of your time, but I am also conscious of the fact that I do not particularly want these questions or the answers to them to be missed. If that is okay with

you, we will write to you. We are very grateful. It has been a fascinating sessions and a very important session for this Committee. Thank you so much for coming.

Professor Michael Clarke (QQ 61-75)

Evidence heard in public Questions 61-75

Oral Evidence

Taken before the Joint Committee

on Wednesday 2 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Stuart C McDonald MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Bishop of Chester, Lord Hart of Chilton, Lord Henley, Lord Strasburger.

Witness: **Professor Michael Clarke**, Retiring Director of the Royal United Services Institute, gave evidence.

Q61 The Chairman: Welcome to you both. We very much look forward to what you have to say to us on what is obviously a very important Bill. I was going to ask a question that could be rolled into one, in a sense, if you have a statement that you would like to make. The question I was going to ask is: what do you think of the Bill? Perhaps you could answer that question and make any introductory comments to the Committee that you might like. You are most welcome.

David Anderson: I welcome this Bill, Lord Chairman. The law in this area has, until now, provided for extensive but vague powers, used in a way that the citizen could not predict and safeguarded by people who, for all their very considerable merits, have not been particularly visible to Parliament or the public. I would single out two major improvements that have already been happening over the 18 months since I started doing my review, *A Question of Trust*, though there is no causal relationship there, of course.

The first is the disclosure of significant and sometimes controversial powers that are already used but that people did not really know about before. You are looking there at bulk collection, the use of bulk personal datasets, the practice of equipment interference or hacking by the Government, and very recently, indeed on the morning the Bill was launched, a very significant data retention power that was previously almost entirely unknown. Many of those disclosures were prompted by proceedings in the Investigatory Powers Tribunal.

The second change is more proactive and visible oversight, in particular by the Interception Commissioner's office, which I single out because it is the office most concerned with the subject matter of the Bill, but also because it operates so transparently. This Bill, as it seems to me, cements those improvements and builds on them. I believe that there is now a complete avowal of significant capabilities, at least in outline. If I am wrong about that somebody was concealing them from me, and, although that is always possible, I do not believe that is the case. What I applaud about the Bill is that, for the first time, Parliament

will have the opportunity, as it should in a democracy, to debate the capabilities that are used or that it is desired to use and decide whether it considers them acceptable or not.

The Chairman: Thank you very much. To both of you, I express the Committee's thanks for the reports you have produced recently, both of which will be immensely important for this Bill, but also for the public understanding of what you just described.

Professor Clarke: I convened a panel at the Royal United Services Institute, which we call the Independent Surveillance Review, consisting of 12 people who represented a pretty wide cross-section of interests, from ex-security chiefs through to people representing civil liberties arguments, practitioners, industry and so on. It was a very well-balanced group, but it was very wide. I am glad to say that our report was unanimous. We struggled with a lot of the issues and tried to take a publicly orientated view. We tried to start with big principles and then go down to the legislation, rather than starting with the legislation, because we thought that would be the most useful thing to complement David Anderson's review and the review of the ISC.

Our review was generally favourably disposed to the present situation, but we felt, as other reviews had felt, that the legislation was not clear enough as it was. This legislation certainly helps to clear that. The oversight regime, we thought, was critical both in warrantry and in the oversight, and it was not that it was incapable of being amended with relatively small changes. The most important thing was that we felt there needed to be much greater public confidence in it; it was not that the public were not confident in it, but they did not know enough about it. We felt that an oversight regime and a warrantry regime that could command more public confidence, which is partly where we brought the element of judicial oversight into the warrantry, would be very important.

The aspect of this Bill that is different from the expectations we had is the scope of what it says about equipment interference and internet connection records. That is controversial but is allowable for within the principles that we articulated. The differences between the Bill and our recommendations are comparatively small. I would be happy to go through them later on, but they are comparatively small. The approach of the Bill is pretty consistent with the review that we arrived at.

Q62 The Chairman: Thank you very much. Before I ask Lord Butler to come in, I will take advantage of being in this seat by asking my other question, which was to come later but touches on what you just described. It is the issue of trust and confidence, which appears to be at the root of all this, but particularly the issue of whether the new system will also produce improved confidence and trust in the agencies and the law enforcement bodies. Is that likely to be the case?

Professor Clarke: It certainly could be the case, because there is generally high public trust in the work of the agencies. They are fairly popular. There is more ambiguity over the work of law enforcement. It is bigger, more complex and covers a wider range of things. There is a degree of cynicism over some of that. There is a degree of increasing cynicism over the role of the state in general to intervene or interfere in the communications of its citizens. It must be a clean and clear oversight regime, with clarity and lines of responsibility that the public can follow. We recommend specifically that whatever arrangement is made for the commissioners should be very outward-facing, should try to publish more material and

enter into a dialogue with the interested public that is wider than the dialogue that has been evident until now. That could be a big element in increasing confidence, not so much in the agencies, which do not need it, but in the police and in the role of Government itself.

On a final point, we began from the principle that this is not a series of technical issues. This represents something pretty fundamental in the bargain that the public make with the Government. In the digital age, this is the tip of a big democratic iceberg, and we have an opportunity now to get it right in a way that will be pretty important to the future of the political bargains we strike. This is one really important bargain that needs to be struck very explicitly and cleanly, as far as we can.

David Anderson: It struck me during my review that the people who need and deserve to be able to trust the system—not just the public, although public trust is very important—and who spoke to me most strongly about human rights, safeguards and the need to be trusted were the service providers, the telecoms companies that give assistance to Governments but are very nervous about being perceived to assist with things that are below board, and the intelligence agencies.

I had a message from somebody at GCHQ, which is probably too secret to disclose, but I will say it anyway because it is fairly innocuous. The reaction I had was, "I hope these new commissioners really make us work hard to prove that what we are doing is necessary and proportionate". If you are trying to recruit people on the pavements of Shoreditch to come and use their technical skills to work for GCHQ, you do not want to be seen to be working in some shadowy grey area where you are dodging in and out of the law; you want to be able to assure them that there is an absolutely copper-bottomed system in place. It is something that everybody wants.

People who are sceptical will be sceptical about safeguards as well. That is the way that people are. Commissioners will be portrayed, initially, as grey-haired old people out of touch. Judges will be portrayed as rubber stamps. That is why it is so important that what they do is transparent and they publicise their work, so far as possible. I would like to see judicial commissioners, for example, not just making wise decisions but issuing guidance, so far as possible public guidance, so that people can see how carefully they are thinking about it. I could go on.

The Chairman: It is hugely important.

Q63 **Lord Butler of Brockwell:** I would like to talk about the drafting of the Bill, if I may. Your two reports made recommendations in strikingly similar words. Mr Anderson's report said that the new law should be drafted in a way that is both "comprehensive and comprehensible", and the RUSI report said that "a new, comprehensive and clearer legal framework is required". Are you satisfied that the way the Bill is drafted sets out the powers and capabilities in as accessible and foreseeable a way as you had hoped?

Professor Clarke: Yes, from my personal point of view. I thought the explanatory notes that came with the Bill were pretty good, but the Bill itself is necessarily difficult because it combines a series of other legislative frameworks, which are very complex. We thought that one of the key elements of this sense of clarity would rest in the codes of practice. We said very specifically that the codes of practice should be written clearly in ways that

ordinary people could understand. The Bill cannot be written in those ways, because it is a piece of statute legislation, but the codes of practice should be clearly written for the more general public. That, to us, would be a very important element of this whole package.

David Anderson: We set parliamentary counsel a probably impossible task, because we asked for a Bill that was comprehensive, and we asked for a Bill that was technology-neutral. It is quite difficult to be technology-neutral and at the same time explain exactly what it is that people are being authorised to do. I entirely agree with Professor Clarke that the code of practice, and not just that but other disclosure, is necessary.

If you are looking at accessible and foreseeable, it seems to me that it is not just about the Bill; it is about getting more material into the public domain as to the utility of some of these powers, in particular bulk, which sits there like an elephant in the room. We have heard discussions about how one can look to see if someone's wife is using the car and whether that is collateral intrusion and so on, but if you are tapping a cable that potentially gives you access to the conversations of thousands or hundreds of thousands of people, you are looking at some very major issues.

Nobody should expect the Government to give away operational secrets or information that is damaging to national security, but it seems to me that we need more in the way of information if this is to be truly accessible and foreseeable. A modest start was made by GCHQ; they allowed me to publish six case studies at Annex 9 to my report. I pressed them unsuccessfully to release more detail, and I was introduced to other case studies they were not prepared to publish. It was a very good start, and I hope more will come.

There are other grey areas that one would not know about from the Bill. This is not a criticism of the Bill, but, for example, can the intelligence agencies use related communications data, which is a by-product of bulk interception, to construct the web-browsing records of an individual? There have been some publications recently suggesting that they might be able to do that. One might think there is nothing particularly wrong with that, but it seems to me it is a relevant thing to know about, particularly if one is discussing internet connection records. If this new, highly regulated power should be introduced for the police to make use of, what about the agencies? Do they already have similar powers in this area?

As to retention, what exactly are the types of data for which the retention powers in Clause 71 could be used? There are all sorts of technical questions about that. One does not expect to see in the answer in the Bill, but Parliament will need to see some answers on those sorts of questions if it is to be able to debate this on a fully informed basis.

Q64 Lord Butler of Brockwell: If I may ask one supplementary question on comprehensiveness, there remains some other legislation with powers of intrusion, such as the Police Act and the Regulation of Investigatory Powers Act. They are not all being rolled into this Bill. God forbid that the Bill should be made even bigger, but do you think that is regrettable?

David Anderson: In a way, we have all stuck to our remit, and perhaps we were too obedient about that. The Intelligence and Security Committee, I do not need to tell you, was looking at the intelligence agencies. You said there should be a new law for the

intelligence agencies and the rest could keep what they had. I was asked to look at interception and communications data, but I was not asked to look at intrusive surveillance, directed surveillance, all the stuff that happens later on in RIPA, so I did not make any recommendations on that. I was not here for Sir Mark's talk, but I have heard him say in other contexts that he thinks that was a missed opportunity and it would have been nice to build some of those powers in as well. One could have built in all the Intelligence Services Act powers.

I suspect there are limits to what human beings can do in a short timescale. I do not often publicly praise the Home Office, whose work I review, but I must say they have worked extremely hard on this. There are people in the Home Office who I know for a fact did not get a summer holiday this year because they were working on this Bill. If one had expected them to do something twice as long, that might have been too ambitious.

Professor Clarke: The ISC, although it dealt only with the agencies, talked about reviewing the whole raft of legislation. We thought that would make the Bill impossible, and certainly impossible to get through in time to meet the requirements of the sunset clause. We stuck to the areas of RIPA and DRIPA and some of the other legislation that we thought was capable of being brought under a single legislative framework.

Mr David Hanson: You have touched on it there. We are talking about the legal framework, but I am interested, before we move on to the legal framework, about the assessment of either of you as to the deliverability of the 12-month holding of records, with both the provider and the Home Office being able to access those records. I wondered whether or not you had a view on that, as well as the legal framework.

Professor Clarke: My own view is that the Home Office, the agencies and the police can certainly have those powers, but they cannot exercise them entirely because of the international nature of the companies they are dealing with. One aspect of these proposals is that they will make it easier for companies who claim that they fall between different jurisdictions to comply with requests that they get from UK authorities, but they will not guarantee it by any stretch of the imagination. This legal framework will help, but in general the power of UK agencies to access as much as they have in the past is declining in any case.

Mr David Hanson: There is also the question of the funding. In the Bill, as we have already touched on, a large sum of money is allocated for support to the providers to deliver the service that the Government are expecting you or subsequent officials to regulate. Have you any assessment of whether those figures are realistic? We will return to that, as a Committee, in due course.

Professor Clarke: We have not made any assessment of that. The Bill came out after we finished our work, so I do not have anything to offer on those particular figures.

David Anderson: You asked about the deliverability of internet connection records. The first thing I would say about that is that the Bill has been a lot less ambitious, as it seems to me, than the old Communications Data Bill 2012, which I know some of the Committee knows very well. In particular, easily the most extensive and expensive feature of that Bill would have been the obligation on UK network providers to retain copies of all third-party

data running over their networks. I think the very modest estimate for that was £1.8 billion, but it was accepted that it would probably be a lot more.

There is an estimate of about a tenth of that cost over 10 years for internet connection records. They have done what I recommended and made out an operational case as to the respects in which the police would find that useful. Does that mean they are deliverable? Not necessarily. I am not seeking to express a view on this, because I do not have one and I am not competent to have one, but there are some serious questions there. Another Committee, I know, is taking evidence on some of these questions. Would it be technically feasible to assemble precisely the types of data that they say are wanted? Would it be operationally worthwhile?

My understanding is that, although no other western country currently seeks to deliver internet connection records, there was an attempt to do something very similar in Denmark. This happened until June 2014, when the law was repealed. One of the stated reasons for that is that the police had not found it as useful as they had hoped. No doubt one can learn from other people's errors, and indeed I have heard that, in Denmark, they are thinking of reviving the idea. But it demonstrates that one cannot just run into these things without a deep technical understanding of how easy it is going to be to isolate and store precisely the types of data that the Government say they need.

Q65 Matt Warman: Going back briefly, I wonder if you could characterise to what extent the Bill, as it is, is a grand but not comprehensive tidying up exercise, versus the introduction of new powers.

David Anderson: For me, the headlines would be, first, transparency, as I said in my opening statement. It is key for democracy that the powers are out there. The second is enhanced safeguards at the authorisation level where intercept is concerned, and not so advanced when you are looking at communications data, and that would be one reservation I have. Thirdly, on powers, it preserves and makes explicit all the powers that are currently used and seeks to introduce one new one, the generation and retention of internet connection records by service providers.

Matt Warman: That makes it sound like you think the bulk of it is an aggregation exercise, with a small number of new powers.

David Anderson: Yes. It is a much more modest exercise in terms of new powers than the Communications Data Bill 2012. The reason it is so much bigger is because they bring into the Bill all these things that nobody had even heard of two or three years ago, but which are now set out.

Q66 Lord Strasburger: One of the powers you have already mentioned is bulk acquisition, which was only avowed on the day the Bill was published. You will be aware that the equivalent of that in the United States is Section 215 of the USA Patriot Act. You will also probably be aware that President Obama commissioned two reviews, in the wake of the Snowden revelations, and they both found that Section 215 powers were ineffective and do not make "any significant contribution to counterterrorism". It was duly repealed, with effect a few days ago, I believe. My question is: would this Bill take the UK into stronger and more intrusive powers when the United States has started to travel in the opposite direction?

David Anderson: It is dangerous and difficult to make international comparisons, although I am not discouraging it, partly because—and this is not a comment on the United States—it is difficult to know exactly what is going on in other countries. I cannot put my hand on my heart and say that I understand the relationship between the Government and the former national telecoms provider in every European country or in the United States. I certainly would not have had any idea five years ago that the NSA had probes in the nine chief US internet companies, as was reported, under the PRISM programme.

There is, as you say, a parallel between a Section 215 power, where communications data internal to the US was gathered in one place, and the power that was avowed early in November, when the Bill was introduced to Parliament. We have seen the suspension of that Section 215 power. I think I am right in saying, although I might be out of date, that there had been rulings to the effect that the power is untenable because it was not sufficiently authorised by Congress. I do not believe that power has been tested against the constitutional guarantees of privacy, so I am not sure that one is necessarily saying that the American courts have gone further in relation to privacy, and indeed there are some respects in which they have not.

Lord Strasburger: Is it possible to answer my question in terms of avowed powers? Would it be true to say that avowed powers in the States are moving in a different direction to the one we are asked to move in with this Bill?

David Anderson: It is difficult to say, even in the United States. They have an executive order, 12333, pursuant to which all sorts of data are collected. It has not yet been reviewed. There is, I think, a proposal to review it, but very little is known about it. I could not tell you what the parameters of that power are, or what exactly it is used to do. You can give the Americans credit for a great deal, certainly in terms of judicial authorisation of intelligence warrants. They lead the world with the FISA court, and there are very few other countries that have attempted anything like that.

In terms of how useful 215 was, I hope that the utility and the proportionality of the newly avowed power will be tested before Parliament. I hope there will be a way of doing that. It may have to be done before the Intelligence and Security Committee. Of course, we already had a power, which everybody has known about for years, under the old data retention directive and now under DRIPA, whereby this sort of data can be retained by service providers. There may be a question as to the added value of retaining possibly similar categories of data in a single place. Is that all about speed of access, or are there other advantages that the intelligence agencies glean from it? It is a very intrusive power, and, if it is going to be justified, it is right that Parliament or Committees of Parliament should be given the opportunity to test its utility.

Professor Clarke: We spent in our panel, given the make-up of the panel, quite a long time thinking about bulk access as a matter of principle. Views differed across the panel. We all eventually came to the conclusion that it was necessary for the purposes of national security and law enforcement, and for all manner of intelligence purposes.

One of the problems in talking about bulk access in this context is that there is a sense out there that only Governments do it, but of course everybody does it. It is part of our digital society. The old phrase is that unless you are one of a very small group of people indeed,

Tesco already knows a great deal more about you than MI5 ever will. Data analytics are used by everybody: by retailers, by charities like my own. Everybody uses data analytics. Bulk exploitation of data is part of our society. When the Government do it, of course they should be held to a much higher standard because of what can follow from their conclusions, but bulk data is a fact of life. Our discussion is not whether we have or do not have it; it is how it is used and under what framework and what circumstances.

Q67 Suella Fernandes: In relation to bulk data, could you briefly give an example of how its possession has helped in intelligence and counterterrorism? I know there are many.

David Anderson: I can do it briefly by referring you to Annex 9 of my report. I only wish I could put names to the terrorists referred to in Annex 9, but I am told that I cannot. A few journalists have guessed, but that is as far as I can take it.

Suella Fernandes: The concern is that individuals who do not fall into the category of criminals or terrorists will have their browsing habits under surveillance and captured under bulk data, so my penchant for very expensive shoes and online shopping will be captured. Can you just describe the interest and the capacity among our law enforcement, intelligence and security services for that kind of information?

Professor Clarke: The safeguards in those cases rely on necessity, proportionality and legality, and the warrant that will now be required for bulk access will be much more specific. It comes down to the ethics of the agencies and the police, and how they operate the powers that they have. We on our panel were very impressed at the high ethical standards in general that apply.

The other great safeguard is the sheer physical capacity. One will be astonished at how little they can do, because it takes so much human energy to go down one track. The idea that the state somehow has a huge control centre where it is watching what we do is a complete fantasy. The state and GCHQ have astonishingly good abilities, but it is as if they can shine a rather narrow beam into many areas of cyberspace and absorb what is revealed in that little, narrow beam. If they shine it there, they cannot shine it elsewhere. The human limitation on how many cases they can look at at once is probably the biggest safeguard.

Lord Strasburger: You mentioned codes of practice. Governments have a habit of holding back codes of practice until long after Parliament has considered the legislation. Would you advise the Committee to urge the Government to publish draft codes of practice so that Parliament can see them while it is considering the Bill?

Professor Clarke: I would strongly advise that. That was a very clear conclusion from our work.

David Anderson: That is right. Of course, many of these codes of practice exist already. For example, an equipment interference code of practice was issued in February. You might notice, when you read it, it does not say much about bulk equipment interference, which is one of the aspects in respect of which some interesting questions are going to have to be asked. I would agree with that.

Q68 **Lord Hart of Chilton:** We have been asking witnesses about the judicial review principles that underpin judicial authorisation, and whether or not they constitute a true double lock system. Could you give us your comments on that?

David Anderson: I find it, as a rule, very foolish to disagree with David Pannick about judicial review. I think he knows more about it than anybody else in the world. I read his article and I agree with it, despite the fact it is not precisely what I recommended. It is much closer to what the RUSI panel recommended.

I would make one point in respect of which I think the double lock, in a sense, is unduly cumbersome. There may have been an echo of that from a previous witness. It is in relation to police warrants, which, in nearly all countries I know about, are perfectly straightforward: the police go to a judge and the judge gives them the warrant. It is not seen as an area where the intervention of a government Minister is necessary. I can see that, in national security matters, different criteria apply. Indeed, I recommended a double lock myself in relation to foreign policy and defence warrants. But in relation to police warrants, which are 70% of the whole and therefore represent 70% of those 2,300 warrants that the Home Secretary authorises every year, it seems to me that one could do without the politician or the Minister and go straight to the judicial commissioner.

Professor Clarke: We thought that the double lock, as the Bill came through, in principle is workable. It is undoubtedly more cumbersome than the present system, but that is probably a reasonable compromise in terms of bringing greater public confidence into the process and aligning us more with our international partners, which will have other advantages in persuading internet service providers to co-operate with requests they could argue they do not need to co-operate with.

Q69 **Bishop of Chester:** I was struck by Professor Clarke's expression: a "clean and clear" process of judicial oversight. Bishops, of course, are appointed in some sense by the Prime Minister, so I have to tread carefully here, but I am glad it does not have to be renewed every three years in my case. I wonder whether it feels right to have three-yearly renewal and the Prime Minister making the appointment, if you want to have a clean and clear process. I would be grateful for your comments.

Professor Clarke: This is a very powerful position and it will require the evident exercise of very high integrity that is unimpeachable. It is not difficult to find people who will do that, but they have to enjoy the confidence of the Prime Minister and the political establishment, and command public confidence as well. When I say "clean and clear", we had in mind the National Audit Office, a big organisation that has important technicians and specialists in it, but also has a big effect at the policy stages and in post-legislative scrutiny. Something approaching that is not unreasonable. The present system has been fairly ad hoc. It works reasonably well, but it could work in a much better way. It would be expensive.

We thought of four-yearly renewals, renewable for a four-year term, but three-yearly is not a bad compromise. I personally would prefer it to be longer, so that somebody could build a greater profile in the work that they do, which the public would get used to.

Bishop of Chester: Five years?

Professor Clarke: Yes, that would be workable as well. One of the important aspects of this role is the outward-facing nature of it. That is not an afterthought. It is important that the work of the commissioner should be outward-facing, seen and understood, in the same way as Her Majesty's Inspectorate of Prisons. It is a really important role and the public should understand what that person does.

David Anderson: I see the advantages of a five-year term, and I see the advantages of making it a single term so that there would be no question of people being careful around the renewal period. I should say that I am appointed as Independent Reviewer of Terrorism Legislation for a renewable three-year term. Did that affect the timing of any fights I might have wanted to pick with the Home Secretary? I do not know; perhaps subconsciously it did.

Another thing to bear in mind is that it depends slightly who you want to do this top panjandrum job. It has to be a senior judge or a retired judge. If you want a serving judge—I am not suggesting that retired judges are not fully vigorous and capable of working six-day weeks, but that is the sort of person you probably want—and if you want to take someone out of regular judging for a few years and then put them back in the system, you might be pushing it to try to go beyond three years. They are familiar with the idea of the Law Commission: you leave the judiciary for three years to do the Law Commission and then you go back. If you are away from it for much longer, you might find people thinking, "Well, that is not really why I became a judge".

Bishop of Chester: And the Prime Minister making the appointment?

David Anderson: I ought to oppose that, I feel, because I understand the argument that it might be perceived as political, but I cannot help echoing what the judges have said to you. These are people who have been independent all their lives. They have been self-employed. They then took a judicial oath to show neither fear nor favour, and they do not. Yes, one could introduce consultation with the Lord Chief Justice, or by agreement with the Lord Chief Justice, perhaps bringing in the Judicial Appointments Commission and possibly some sort of parliamentary hearing. For the purposes of public perception, that may be a good idea. I suspect you would be better judges of that than I would.

Q70 **Stuart C McDonald:** First of all, I have a supplementary on a couple of things you said earlier. You both referred to a degree of public scepticism and cynicism, which largely arises because we are aware of all sorts of capabilities and practices being used that we had never heard about. How do these provisions prevent that from happening again? How can we ensure that things are not going on that we should know about but do not?

Professor Clarke: Partly because this Bill will tighten up a lot of powers and they will all be in one place. One of the reasons for some cynicism among those who took an interest in this is that they thought, as there were so many different legislative frameworks that the agencies or the police could use, it was almost as if there were loopholes that would allow them to do what they wanted. That was part of the basis of the cynicism. That would not exist to anything like the same degree under this legislation, so the tidying up and the clarity with which it could be presented, with the oversight, would provide a much greater reassurance.

As David said earlier on, those who will not be convinced will not be convinced by it. In a way, the battleground in terms of public confidence is the more average person, who feels that at least they know there is a process. They may not know the details of it, but they did not even know there was a process until last year. At least if they know there is a process, they can take some interest in it and feel confident that the people operating that process are operating it independently.

David Anderson: In recent months, it has been the Investigatory Powers Tribunal that has been the main battering ram in securing avowal of programmes. That may conceivably be something of a one-off. I regret to say this, because I do not condone what Mr Snowden did, but it was information allegedly disclosed by Snowden that prompted some of those cases and eventually prompted avowal by the Government. I do not think that is a good model on which to proceed for the future.

The key has to be the commissioners. I have very high regard for what the commissioners have done, but I remarked in my report that it was not the courts, commissions or committees of London that disclosed to the British people what was going on; it was the revelations that originally came from Mr Snowden. That is not the way it should be. I hope one advantage of this big new commission, with the technical expertise, with the weight to get inside the agencies and work out what is going on there, is that these things will not come as surprises, and, if these commissioners feel there is something important going on that ought to be disclosed, they will write to the Prime Minister, as I wrote to the Prime Minister about the power that was disclosed on the morning of the Bill. I suspect they will find, as I found, that there is no resistance whatsoever to doing what is clearly right.

Q71 Stuart C McDonald: That is helpful, thank you. You have suggested that international comparisons might not be all that helpful. Nevertheless, I was planning to ask you about international comparisons, so I will do so. Are there ways in which this Bill, perhaps in its provisions relating to oversight, data retention, bulk collection, goes further than what similar countries have put in their legislation?

David Anderson: If one were taking a very general look at it, this is a very extensive set of powers, certainly by western standards. We are a major SIGINT power. That is reflected in the powers and that is why we need such strong safeguards to go with them. Moving away from those glamorous agency-type powers, one is also looking at things like the retention of quite basic call data by service providers, largely for the use of the police and other users of data.

Possibly reflecting the public mood in this country, although there are safeguards, they are not as tight as they are in some countries. For example, in Germany they have just reintroduced their own data-retention law. They require the data to be kept for four weeks, whereas the idea here is it would be held for 12 months. The Germans are going to require judicial authorisation for anybody who wants to look at it, which people are saying over there is going to be very cumbersome. Jo Cavan told you that there were half a million applications to look at communications data last year. Plainly, one could not ask people to go before a judge on each of those occasions.

As a nation, we seem to be less concerned about our own privacy, at least vis-à-vis the Government, than some of our neighbours in Europe and indeed across the Atlantic. That

is probably reflected in what is a pretty strong suite of powers. That is why we need a strong suite of safeguards to go with them.

Professor Clarke: The only thing I would add is that there is an idea around this legislation that our country that has a high reputation in intelligence matters. We have a global intelligence capacity that not many other countries have, and that plays to our advantage most of the time. This represents a modern piece of legislation and, if the oversight capacity and the confidence that can be built into it are there, and if we put enough resources into it, it can be a world leader in legislative provision. One of the aspirations behind this thinking is that it would act as a very good example of how to get the balance right for a power that wants to retain high intelligence capabilities.

Q72 Stuart C McDonald: I have one final question. Correct me if I am wrong, Mr Anderson, but I think you said earlier that you some reservation about provisions relating to communications data. Could you expand a little on that?

David Anderson: One of the submissions I heard from a lot of people is that you can tell more and more these days from communications data. It is not any longer just the writing on the envelope; it can be the location data showing where someone was. Quite a lot of personal information can be detected, particularly when bulk personal datasets are combined. My reaction to that was not to say you have to bring in a judge every time. You cannot require a judge to authorise a simple reverse lookup when you are looking for a lost child in an emergency. But I said that there are categories of communications data requests that ought to be independently authorised, so why not by the commissioners?

I gave some examples—people looking for sensitive information about whom a lawyer might have been talking to and other novel or contentious cases, which is a concept that the commissioners would have to build up over time—that, it seemed to me, ought to be authorised by the commissioners. The commissioners ought to be able to put out guidance so that people would know the principles on which they were acting and you would have a principled framework governing these things, instead of the opinions of lots of different designated persons in different places.

Behind that idea was the way the law seems to be moving in Europe. There was a case, Digital Rights Ireland, last April, saying that you needed a prior independent authorisation even for quite simple communications data requests. The High Court this year decided that DRIPA was invalid because of a failure to give effect to that requirement. The Court of Appeal retrieved the position, from the Government's point of view, a couple of weeks ago by indicating that it was going to ask the European Court of Justice what it really meant. It will probably be 18 months or so before we find out the answer.

There is quite a lot of pressure from a number of angles. There were not many disappointments, to be honest, and I think they gave effect to the great majority of my recommendations and those of RUSI, but one reservation is that they did not do much to improve the authorisation of communications data, not just by police but by others as well.

Lord Butler of Brockwell: To follow up on that, how confident can you be that this Bill is going to pass the requirements of European law?

David Anderson: It is a very sensitive question, because the Court of Appeal has decided it is going to ask the questions of the European Court. I do not believe the questions have yet been finalised or sent off. If one restricts oneself to what has happened in other countries, my understanding is that around five constitutional courts and some other courts, in countries such as the Netherlands, Belgium, Slovenia and Austria, have already decided that national laws based on the data retention directive, as ours was, are not valid. The High Court here said the same thing. The Swedes were made of sterner stuff; they asked Luxembourg the question, and so did our Court of Appeal. Trying to predict the results of litigation is a mug's game and I am not going to succumb to the temptation.

Q73 Matt Warman: You both implicitly mentioned the idea that this is the UK leading the world on the kind of legislation that we are going for in this area. The other side of that argument is that, if it is taken by regimes that do not share our judicial oversight and our values, it could essentially be misused. Is it ever reasonable to draft our legislation in the light of what another country might do with it for good or evil?

Professor Clarke: I would say no, because our legislation is for us. In a way, this will provide a model of legislation, because of the oversight provisions and independence that is meant to be built into that. If other countries that did not share the same democratic values imitated this but in a way that was a façade, that would be fairly clear.

One thing that we say in the RUSI report is that a start can be made by bringing together countries in the OECD and some of the like-minded liberal democracies. We need to create a much bigger consensus on the way in which legislation should handle this increasingly complex relationship between citizens and government in the digital age. This legislation could provide a basis for discussions with a lot of our partners. There will, of course, be quite big differences, because there are big cultural differences between the way Germany, the United States and Britain, let alone France, see these issues. There is a case for saying that a piece of model legislation would be a good example, and we should not try to second-guess what less democratic countries would do in response to it.

David Anderson: We are not at the privacy-minded end of that spectrum, but it is very important that we reach out and make our law understandable to people who are in a slightly different place. That is because this law has a huge extraterritorial reach. We assert the power to do a lot of things beyond our own frontiers. It is also because, as Professor Clarke was saying, to the extent that our law enforcement and intelligence agencies are seeing the world going dark, that is, in part at least, because there are internet service providers in other parts of the world, particularly the United States, that are wary of accommodating foreign Governments in their requests for information, particularly if those Governments do not respect what they see as the safeguards available in the United States, one of which is judicial authorisation.

I do not put it on the basis that we should set a good example for the rest of the world, although it would be an admirable thing if we could. I put it on the basis of self-interest, producing a law that is acceptable to the rest of the world, whether you are looking at courts in Luxembourg or tech companies in California, because that is the way to advance our own interests and to make sure that the people who need it can get the information they need.

Q74 Matt Warman: Finally, one of the crucial extra powers is the retention of internet connection records. Do you feel that that case has been adequately made publicly? Do you feel that the public have got behind that yet?

David Anderson: The Government have produced a 24-page operational case, as I recommended they should. I did not recommend 24 pages, but they have produced an operational case. They made out their case for three reasons why the police and others might want that information. That is now free for committees to interrogate, and no doubt you have started that process already. As I said earlier, the question marks that still remain in my mind relate to feasibility, cost, security of storage and all these other matters.

One always imagines the police will ask for all the powers they possibly can, but they are very conscious, particularly at a time of financial stringency, that they have to train people to use these new powers. They need to devote budgets to doing do. If it turns out to be a bit of a damp squib, as may have been the case in Denmark, they will feel they have wasted their money, so it needs a cool, hard look. I applaud the Government for doing that in relation to third-party data retention, which was said to be essential back in 2012 and which is now not essential anymore because it does not feature anywhere in the Bill. That has saved the country a very great deal of money.

I am not saying that internet connection records are in the same basket. I can certainly see how useful they could be, particularly in IP resolution and in tracing the fact that people have been using communication sites. How easy is that going to be to achieve technically, when nobody else in the world yet really does it? I do not know.

Professor Clarke: There is a principle behind that, which we talked about quite a lot in our panel. Is it the case that, in principle, law enforcement should have a right to try to go wherever the criminals are, or are there some areas in which we say, even if criminals inhabit them, the Government do not have a right to go? There is no easy resolution to that issue, other than to take a view, either yes or no. That, in a sense, is what we are talking about. Whether the adequacy of internet connection records as an investigative tool is correct, we do not know. We just do not know how useful it will be, but it does raise exactly that principle. Do the Government have a right to go anywhere where the criminals might be?

Q75 The Chairman: I have one final question, which relates to the first one I asked. You are satisfied with the draft Bill, by which I understand that you are satisfied that the major recommendations of both your reports have been taken on board.

David Anderson: I have not totted them up. I can say that around 90% or more of mine have been wholly or substantially taken on board. Although my report, I am afraid, is very long, most of it is descriptive and the recommendations themselves fit into about 20 or 25 pages, whereas this Bill is closer to 200. For me, the challenge is going down a level into the detail and seeing whether those who have applied themselves to that detail have made all the right decisions.

Professor Clarke: As Chair of the RUSI panel, I can say that the Bill met most of our expectations in terms of the recommendations that we made. Also, at the end of our report, we elucidated 10 principles and said any future legislation must meet those 10 tests.

I would recommend you have a look at those tests. I think the legislation meets most of them.

The Chairman: It has been a fascinating session. Thank you both very much for coming along. I am sure you will be interested in the recommendations we eventually give the Government. Thank you very much indeed.

Jesper Lund, Chairman, the Danish IT Political Association (QQ 234-249)

Evidence heard in public Questions 234-249

Oral Evidence

Taken before the Joint Committee

on Wednesday 6 January 2016

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins, Suella Fernandes MP, David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Bishop of Chester, Lord Hart of Chilton, and Lord Strasburger.

Witness: **Jesper Lund**, Chairman, the Danish IT Political Association, gave evidence.

Q234 **The Chairman**: A warm welcome to you both. Welcome to the British Parliament. We are dealing with a very important piece of legislation that we have been asked to look at by the House of Lords and the House of Commons. We are very grateful to you both for travelling to give your views on some parts of this legislation, and I thank you both very much indeed for coming along. I shall start the question session with a very general question to you both. If you wish to make general points about the Bill it may be appropriate for you to do it at this point. Do you think that this Bill is necessary at all, and do the provisions of the Bill strike the right balance between privacy on the one hand and security on the other, which is the eternal question?

William E Binney: First, I thank the Committee for giving me the opportunity to come and give testimony. I hope I can help you with some of the issues you are discussing in this Committee. My big objection with how NSA, GCHQ and the law-enforcement agencies affiliated with them deal with data is fundamentally about the bulk acquisition of data of any type. When I became the technical director of the world analysis and reporting group at NSA, which had about 6,000 analysts and was responsible for reporting on every country in the world, I had to look at the major problems that they were facing and try to figure out ways of solving them. I took the position in 1997, when the big explosion of digital communications was occurring, so the biggest issue I had to face was that explosion and how our NSA analysts were dealing with it. This was also true at GCHQ. GCHQ and NSA basically do the same thing, so they co-operate very closely. If one has a problem, the other does, and they have the same problems. The issue was that our analysts, even back then in the 1990s, could not see how to resolve issues around the world because there was too much data for them even to look at. That was before we had the bulk acquisition of data we have today. Back then, we were collecting the smallest lines of communication. We could not deal with the fibre rates. We did not invent that. A little lab I had, the Signals Intelligence Automation Research Center, invented the ability to pull back together and recompile everything going at fibre rates in 1998. At that point, we deployed that, creating problems that were orders of magnitude greater for the same analysts because they were still doing dictionary select routines that would look through data and pull out anything that matched the dictionary. That basically pulled in everything, dumping all that data on the analysts, so they could not see the forest for the trees.

That was the fundamental problem. The way I approached that was to ask what was the fundamental issue that would solve the problem. It boiled down to looking at the metadata that was used to transport the data around the networks, and there were only two networks to deal with. One was the public switch telephone network, using cell phones, landlines, satellite phones and so on, and the other was the internet. In the case of cell phones, they are run by the International Telecommunications Union and are organised into nine zones around the world. The internet is run by ICANN and IANA. IPv4 and IPv6 basically tell how data is routed across the network, where the terminals are and who they are. It is the same as a telephone number, except the internet is divided into five zones, not nine, and the numbering is blocked and allocated in sections of blocks. I have information on that that I would like to share with the Committee so that members can look at it at their leisure to help them understand the issues.

Using that data gave us the ability to build social networks for everybody and see how they relate in the world and to use that as an upfront filter to sort out the data as it is passing the point of collection or of access. Our process allowed us to see into the massive amount of data. Our initial objective was to run at the order of 10 terabytes a minute, which, to give a scale, is several Libraries of Congress every minute. We were going to scale up from that because that is the order of magnitude of what is going on in the world of communications today. From that, we built this entire targeted approach. It gave us the known targets which we centred on, and then we used the social networks, the defined zones of suspicion around them, to give us a very finite number of targets to look at and pull out data. We were getting ready to apply other rules, but did not do so at the time. For example, if you had a satellite phone that could be located in the mountains of Afghanistan or the jungles of Peru, you fell into the zone of suspicion, so you were pulled in as a part of that. All this was run by code, automatically. We had no people involved in this process. That was what the Signal Intelligence Automation Research Center was all about. This was all done for about $3.2 million. That was the entire cost of that operation. It showed that you had to get away from dumping bulk acquisition on your analysts because that makes them fail, and that is consistently what has happened.

That is what I objected to from the beginning of this process at NSA. That has made its analysts fail, and they have failed consistently since 9/11 and even before then. My thrust is against bulk acquisition of anything. Let us do collection, analysis and reporting smartly. Let us do it in a directed way. That will give privacy to everybody in the world because you do not take in their data. You can filter it upfront. You can even sessionise it and recognise it at the packet level. You do not have to do it at the full reconstructive session. That is my thrust. The Bill should really address bulk acquisition and terminating that. That is really what I think.

Q235 The Chairman: Thank you so much. Mr Lund, would you like to give your views?

Jesper Lund: Thank you, Lord Chairman. I am glad to be here and to give evidence before the Committee. I will focus on internet connection records in my opening statements because in this area I have serious concerns about privacy and efficiency. This is probably an area where the Bill does not strike the right balance between the two. It is tempting to compare ICRs with phone bill or call detail records, as they were formally called. This was also done in Denmark when our ICR scheme was introduced about 10 years ago, but there are a number of differences. The internet is simply not as structured as the telephone

system, where you have a line in use whenever two people are communicating with each other, so you have a caller and a call party and a duration of the call that can easily be registered, and is usually registered for billing. For the internet, it is not as straightforward to do something similar and it is certainly not something that exists today. So, if you force communications service providers to do this, internet connection records will have to be formally defined, equipment will have to be purchased, and the data that you are going to get will probably not be what you would expect from a law enforcement perspective if you think about two people communicating via Skype or Facebook because the internet is a stateless system. Every communication is broken into packages which are transmitted independently. In principle, you can retain some information about these packages that are transmitted across the internet but it is going to be a really large database and highly unstructured. There is going to be a needle in a haystack problem every time you use this data.

In terms of privacy, since so much goes on on the internet nowadays, you are essentially going to store everything about the activity of British citizens, at least to the extent of their activity on the internet. Even if only a small fraction of that data will ever be accessed, citizens will still have the impression that, when they do something on the internet, information is retained about it, which was not the case before, so there is a substantial proportionality issue here that I think should be addressed. In terms of necessity, internet connection records may not be as useful as you would think in the first place. I am sure we will come back to this on questioning, but the Danes' experience, which was based on the same objectives as this Bill, ended up with the conclusion that internet connection records were really not useful for law enforcement work. They were barely used and after seven years a similar system, which, I should point out, was perhaps less ambitious, was scrapped in Denmark. However, it was less ambitious because of cost, so doing something that could potentially be better would also be more costly.

Q236 **Suella Fernandes:** I want to look at the comparisons between the Danish experience and what is proposed in this Bill. Mr Lund mentioned cost. Would you agree that one of the big differences was that in Denmark the equipment cost of data retention was borne solely by the communications service providers, whereas there is a very different approach under what is proposed in this legislation?

Jesper Lund: Yes, I understand your question. It is true that certain compromises were made in Denmark because the cost of the equipment was borne by the communications service providers. The limitations that have been pointed out by the Ministry of Justice in its self-evaluation report affect only about half of the customers that the internet connection records are concerned with, so if there was a case for using this system it could certainly have been proved. As regards the other half of the customers, where problems turned up at a later stage because of some compromises that were made early on, some but not all the customers were affected, so if there was a case for using internet connection records I think they should have been able to prove it with the Danish system, even given the compromises that were made.

Suella Fernandes: Would you agree that cost was a key factor in the options used, whereas in the UK legislation that cost is not such an important factor?

Jesper Lund: Perhaps I should explain to the Committee what compromises were made. The main compromise in Denmark was that communications service providers were allowed to retain internet connection records at the boundary of their network, which is normally not a problem. It was not seen as a problem in 2005 because at that time the sharing of IP addresses was fairly limited. But since we have had more devices using the internet, especially smart phones and tablets which need lots of IP addresses, we have sharing of IP addresses and when the connection is done at the boundary of the network it is sometimes impossible to distinguish between different customers. That was certainly a limitation and was a factor in the limited effect of the Danish system. I should also point out that it affects only roughly half of the customers who were subject to internet connection record retention. I say again that if there was an operational case for using internet connection records in police work, the Danish law enforcement authorities should have been able to prove it for the other half of the customers where these limitations should not really be a problem.

Suella Fernandes: Just lastly, on a point of comparing capabilities, would you agree that the UK has extensive experience of delivering central systems and in training law enforcement and technical capability, whereas the evidence has been that it has been more limited in Denmark?

Jesper Lund: I certainly agree about that. It is true that the evidence for using internet connection records in Denmark is not so good. However, there is other evidence on the use of other types of data retention by the Danish police which shows that it is highly professional and done quite well, especially call detail records and locating information from mobile phones, so I would not say that the Danish police lack technical skill in using data retention for their work. My interpretation would be more inclined towards saying that internet connection records are simply not as useful as was thought initially.

Suella Fernandes: Mr Binney, how would you compare the capabilities between what is proposed in this Bill and US powers?

William E Binney: Well, the US has an awful lot of resources around the world. I mean it has implants on switches and servers around the world; the latest publications stand at over 50,000. I believe that with the latest collection of SIM cards that GCHQ did, plus some other stuff that NSA does, they probably have millions of other access points. That is really intruding into the system in an active way on a massive scale. But again, the end result is so much bulk data that analysts cannot figure out what they have. That is the real problem. The problem of doing intentions and capabilities predictions—that is, the threats from attacks and so on—is an analytical problem, not a data problem. It takes data to figure things out but you have to be selective in it because the selective targeted way gives you a rich environment of information to figure out what attacks are going to happen. If you put all that bulk data in, it covers it up and people cannot see it. That is the problem they are having today; that is the problem they have always had. That is why we did the programme to try to solve that back in the 1990s, and that is when we did solve it.

Q237 **Victoria Atkins:** May I just clarify Mr Lund's evidence? You have told the Committee that certain compromises, to use your word, were made. Am I right in understanding your evidence that those compromises meant that 50% of customers were essentially in the dark—

they were black—to the security services through the collection of the ICRs you have described?

Jesper Lund: Yes, I am not sure that it was precisely 50%, but in all cases IP addresses were shared, so it was basically everyone who accessed the internet from a mobile device.

Victoria Atkins: You used the word "compromise"; another way of putting it is that the system employed by Denmark, with the costs borne by CSPs, is in fact half as effective as the system proposed in this Bill. Would that be a fair way of putting it?

Q238 **Victoria Atkins:** You used the word compromise; another way of putting it

Jesper Lund: That is one way of putting it, but it is still the case that for the other half of the customers, these limitations and compromises should not really affect the potential for using internet connection records for investigative work, even in those cases where the police are unable to come up with realistic cases of the use of such connection records.

Victoria Atkins: But if the system is so flawed in the first place that they cannot locate 50% of their market, it is not very surprising that they rather lose faith in the system, is it?

Jesper Lund: Maybe not, but I would still say that for what we call fixed lines for internet access in private homes, these problems, because of collection at the boundary of the network, should not really affect the potential usefulness of internet connection records. Still, neither the police nor the Danish security and intelligence service, which is our version of MI5, have been able to come up with concrete cases of using internet connection records to determine what communication services people have accessed, for instance, which was a deliberate goal. The Danish police have stated in evidence given to the Danish Parliament that what they usually do instead is seize the laptop or smartphone of the suspect and investigate that device, instead of getting access to internet connection records. They did not give their reasons for doing that but presumably it is because of the extremely large data set that they would get if they retrieved internet connection records from communication service providers and they would be searching for a needle in a haystack, whereas presumably the information that can be obtained by seizing the suspect's laptop or smart phone and searching that is of much better quality for the police investigation.

Victoria Atkins: That is two issues, if I may say so, and indeed law enforcement in this country seizes devices where it is able to. However, the devices are not always available, and we have heard from other witnesses about that. I just want to pin you down on the point about the differences between the Danish and British systems. If a terrorist or a paedophile happens to be in the dark 50%—in other words, the 50% that is not available to Danish law enforcement—then they are not going to be detected under the system as deployed under the Danish method. Is that right?

Jesper Lund: That is true for the system of collecting internet connection records that is no longer in place.

Victoria Atkins: If I understand your evidence correctly, the reason why these compromises happened in the Danish system was that the commercial service providers were bearing the

costs, and they wanted to get away with paying as little as they could. Would that be a fair analysis?

Jesper Lund: I would say yes, but in the end the Danish communication providers are of course going to do what they are ordered to by law, so if Danish politicians had really wanted a more extensive system they could have obtained that. The cost of the Danish system, if you take the cost of the system that is no longer in place and scale it up to the UK, is something between £15 million and £20 million per year. Multiply that by 10 and you have something like what is budgeted for the British system under the Bill, with the compromises that in the end will no doubt have some negative effects.

Victoria Atkins: So that I am not asking you questions that do not fall within your expertise, do you have any knowledge of the business relationship between commercial providers in the UK and law enforcement? Are you aware of how well they work together?

Jesper Lund: No, I am not.

Victoria Atkins: No. Looking again at the Danish situation, then, is it fair to say that the relationship between the commercial providers and law enforcement is not as strong as has been indicated in the course of these evidence sessions? We have heard from Vodafone and others about the interactions that they have with commercial providers here in the UK.

Jesper Lund: Danish communications providers follow the law, of course. They also work together with the Government on setting up systems that are manageable. So the history of the Danish system for the collection of internet connection records was not just a matter of cost; it was initially a matter of the Minister of Justice wanting something that was technically unfeasible. I see signs of the same thing in this Bill. For instance, it is mentioned that an internet connection record could be the destination IP address or the server name. It is certainly possible to define internet connection records in terms of both IP addresses and server names but, in terms of complexity, and hence of the cost of running these systems, there is an order of magnitude in the difference between requiring communications service providers to retain the internet protocol address and doing the same for the server name. The first is pretty simple, but asking them to retain the server name is asking them to do deep packet inspection because the server name is not really available to them. What they get is a packet and an IP address, and then they transmit that packet to the IP address. To get the server name they will need to do some form of deep packet inspection, which is a lot more costly than simply retaining the server name. There was collaboration between the Danish telecommunication industry and the Ministry of Justice, to the benefit of both parties.

Q239 **Lord Strasburger:** Good afternoon, gentlemen, and thank you for travelling as far as you have. I think I have a pretty good idea how you are going to answer this question, Mr Binney, but I will ask it anyway. Is there a good operational case for the provisions in the draft Bill on bulk interception, bulk acquisition of the collection of communications data and equipment interference?

William E Binney: My short answer to that is no. The reason for that, again, is that in each of those cases, no matter what you do, you are capturing so much data. For example, GCHQ alone wants to collect between 50 billion and 100 billion records per day on certain aspects

of communication. That dumps 50 billion to 100 billion events or activities on all their analysts, but they may produce 1,000 or 2,000 analyses at most. If they use the standard approach of doing a word search, which is what the NSA does but is the wrong approach, what happens is that when they look at content from the internet, from transcribed phone calls or indeed from anything by either machines or people, they get so many matches it is like getting a Google return—every time you submit a Google query you could get 100,000, 1 million or more returns—and that is just from the input for that day, and every day is the same. That means that the analysts cannot get through the material, which means that they fail to see the threats. The end result is dysfunctionality among the analysts and no prediction of intention or capabilities, no stopping of attacks, and people die. Then when they die, you find out who did it, and then you focus on those people. That is when you do the targeted approach, like the French are doing now—they are going after people and raiding them because they went after the people who had done the attack and looked at who they had relationships with from the bulk acquisitions that they had. They could have gotten all that data upfront through a targeted approach, and could have had the opportunity to stop the perpetrators before the attack. That has been true in all these cases. We have even proved that it was true with regard to 9/11. The NSA could have done that too.

Lord Strasburger: The Home Office argues that it is essential in the modern world to give the agency every means available to find needles in haystacks, in order to keep us safe. Is that correct?

William E Binney: My response to that would be that it is not helpful to make the haystack orders of magnitude bigger, because it creates orders of magnitude of difficulty in finding the needle. That is really the issue. Using a targeted approach would give you the needles, and anything closely associated with them, right from the start. That is a rich environment to do an analysis on, and it would help the analysts to succeed in predicting intentions and capabilities.

Lord Strasburger: Would any alternative approaches to these bulk powers be more proportionate and effective?

William E Binney: Yes. It is called the targeted collection approach, using the ability to look into the data that we currently have with devices such as Narus and Verint and various other commercial devices, and then giving it sets of targets to look at as well as defining zones of suspicion around it. That would manage all the data input and selection or collection out of the data flow. It means that you get that smart, rich environment for analysts to look at and analyse, and it costs a minuscule amount—probably one-hundredth of what they are spending now.

Lord Strasburger: Does the presentation that you have given us refer to what you call targeted collections?

William E Binney: Yes, and it shows how to do them.

Q240 Bishop of Chester: I find the evidence this afternoon fascinating, because in a sense you are attacking the engine room of the Bill. It is like an Exocet targeted on it.

William E Binney: I always do things in a targeted way.

Bishop of Chester: I imagine this as an aircraft carrier. It will be a very big one when all the data comes in, and it is vulnerable. Let us assume that I am convinced you are right—I am certainly very interested in what you are saying. Why do you think that the British Government, with all their GCHQ experience, their relationship with the NSA et cetera, have taken this approach, which is so diametrically opposed to what you advocate?

William E Binney: I think I know exactly why. They took it because the NSA did. The NSA did it because of contractors and the interests of contractors in getting money and feed-in. There was an awful lot of money upfront, like $3.8 billion, to start the Trailblazer programme, for example. If you want to look that up on the web, it was the one where they started to do capture of data on the internet alone. There were other multi-billion dollar programmes that followed it and were associated with it. So there is an awful lot of money behind the scenes that the contractors wanted to feed on. They all lobbied for this approach because it took so much more money to do. That gave them the opportunity to get more contracts and feed-in. I called that relationship between NSA and the contractors an incestuous relationship because people would retire from NSA and go work for the contractors and use their influence to get contracts and things like that. That was the way NSA took it. I publicly accused it of this, of trading the security of the people of the United States and the free world for money. This is why it did that.

Q241 **Mr David Hanson:** I am interested from both of you what the balance is. You indicated that bulk collection and its analysis has some potential value but it is needle-in-haystack value. On the same side, we have the targeted approach, which would follow through particular leads. Currently, what is the balance in terms of government activity on that?

William E Binney: Currently, there is not too much of a balance unless there is an attack, for example the recent attacks in Paris. Take those two attacks as the case in point. After the first attack, they went to bulk acquisition. How much good did that do them in helping to prevent the second attack? It did not help, but they started getting and finding people once they found out who did the attack and focusing in on the data they already had accumulated on those people, which they could have got originally from a targeted approach upfront instead of waiting. By doing that, now they find other people and are potentially stopping future attacks.

Mr David Hanson: We have had evidence from police and other agencies saying that the targeted approach cannot work now because, effectively, a range of material is in Facebook, Twitter, the dark net and other forms of media. The purpose of bulk collection is that we do not know who is involved in that until there is a lead. The lead follows through to accessing bulk collection material. Is that valid?

William E Binney: I understand that, but with the dark web, when you put a tap on the fibre line, you get the entire fibre line—whether it is the dark web or not. If it comes across the fibre, you get that data.

Mr David Hanson: But the justification that we are getting is that to have an effective targeted approach to people involved in or accessing terrorist, criminal or paedophile activity, or whatever it might be, the agencies need to have access to any record. Any record means

anybody in this room's record, but actually it would ultimately only focus down to the record of one person in this room because they were the person we were interested in.

William E Binney: I understand that that is the objective of intelligence, too, to be able to do that. Again, the issue is doing automated approaches for analysis of the data upfront. That really gives you the ability to sort that thing out. For example, if you want to look at terrorism, you want to look to networks that use the internet or phone to communicate. You look for zones that connect certain parts of the world, such as certain countries. You can automatically do that with software, which is what we were doing, but they did not particularly opt for. That was their option and they picked it because of the money involved. You can automatically do that with software but when you reject the smart approach to targeted analysis, processing of data and analytic processing, you reject the opportunity to solve those problems upfront. Then you end up getting only bulk data because it is, "I know nothing so give me everything". That is what you are saying when you do bulk collection: "Give me everything so that I have the opportunity to find out".

Mr David Hanson: I think that we had it put to us that it is, "I do not know everything but I need to access something which I cannot currently access".

William E Binney: I would say that that is false. They can currently access anything they want. When you tap a fibre, you have access to everything. When you go to an ISP or the telephone company, they have access to the entire network. You can tell them to give you any number or any switch they have got, or they can use the implants they already have in place to do that. That is not an issue.

Q242 **Victoria Atkins:** Just to be clear, Mr Binney, it is 15 years since you worked for the NSA, and your security clearance was removed before you resigned in 2001.

William E Binney: I did not resign; I retired.

Victoria Atkins: On leaving the NSA, you co-ran a consulting company providing intelligent security computer analytics. Is that correct?

William E Binney: It was called Entity Mapping, LLC, yes.

Victoria Atkins: I do not have any view on this, but when you describe an "incestuous relationship" between NSA and contractors because employees from the NSA go to contractors, it could be said that you profited from your role at the NSA after you retired.

William E Binney: We never attempted to get into contract with the NSA. We only did it with NRO, CIA and Customs and Border Protection.

Victoria Atkins: What is this document?

William E Binney: It is the way to do targeted analysis and reporting, and gain a rich environment for an analysist to get data off the network.

Victoria Atkins: Is it a computer program?

William E Binney: It is in the form of a computer program, yes.

Victoria Atkins: And who owns it?

William E Binney: The company name is TDC, the Technology Development Corporation, which has the set of software to do the sessionising of the data. We had at one point the software to do the analysis of it but we left that with the Government.

Victoria Atkins: Just so we are clear, do you have any commercial interests still in this area?

William E Binney: No, I am not in business now at all.

Victoria Atkins: Okay, thank you. Following on from David Hanson's questioning, we heard from a number of law enforcement officers and security services witnesses who are at the rock face now, not 15 years ago. Their evidence has been that they need these powers. Are you telling this Committee that each and every one of those witnesses is wrong, and indeed possibly misleading the Committee?

William E Binney: I guess I am.

Q243 **Shabana Mahmood:** I want to come back to internet connection records and you, Mr Lund. Obviously, we have had quite a long discussion already about the Danish experience, its usefulness and your opinion of that. First, I want to touch back on this point about the 50% data that were not available in the Danish system, which I think you defined as everybody who accessed the internet on a smartphone.

Jesper Lund: Yes

Shabana Mahmood: So the argument is that the Danish example is not helpful because there was this whole bunch of data that could not be accessed and therefore it does not tell us anything about what we are trying to do with internet connection records in this country. But is it not the case that even if in the Danish experience they had been able to get that 50% of smartphone data and had complete coverage, as our system attempts to do, that data would have been potentially mostly useless because of the problem of constant connection and the fact that on smartphones the apps that police and other people would be most interested in are on a background app refresh and therefore constantly connected to the internet, which tells you nothing about when it has been activated? Would you agree with that?

Jesper Lund: Yes, you would be able to see that a person, for instance, uses Facebook or Facebook Messenger, but you would probably not be able to see when that person is communicating with Facebook Messenger because there is constant communication in the background between your smartphone and the servers at Facebook.

Shabana Mahmood: So that additional 50% that could have been collected but was not is probably not very useful anyway.

Jesper Lund: It is always hard to make statements about hypothetical situations, but I would still say that if there was a rational case for using internet connection records, Danish law enforcement should have been able to prove that using the other half of the customers, where these limitations were not a problem.

Shabana Mahmood: Was there anything positive about the Danish experience? We have heard a lot about its problems. Did anything come out of that experience that you or other people in Demark have found useful?

Jesper Lund: No. Lots of data were retained for seven years, and Parliament was told several times that they were extremely useful for the police, but in the end, a self-evaluation report by the Ministry of Justice—not by some critical NGO that makes up a story about this—was not able to come up with a single operational case where internet connection records were used in investigating criminal activity. Even the Danish security and intelligence service, which was asked only about the quality of evidence, not about operational cases in an anonymised form, said they were of limited use to it. Initially, the Danish security and intelligence service, the Danish equivalent of MI5, was the mastermind behind our internet connection records system.

Shabana Mahmood: Thank you, that is helpful. From your submission, there is a suggestion that there are discussions about future proposals, possibly concerning internet connection records, in Denmark mark 2. What is happening with those discussions and what might a mark 2 scenario look like?

Jesper Lund: The Danish police and the Ministry of Justice want to get away from the simplified version of doing collection at the boundary of the network. They want to do it closer to the customer so that the information can always be associated with a specific customer, even when you have sharing of public IP addresses. The Danish telecommunications industry is highly critical of this because it will increase the cost substantially. I do not know precisely by how much, but it is by so much that the industry is opposed to it. If you translate that to the British scale, that would be greater than the budget that has been set aside for your internet connection records, the £170 million over 10 years. If they do that, it will be equally effective for fixed lines, where you do not have sharing of public IP addresses, and for mobile phones where you do. My suspicion is still that it will not be useful at all in the end, and that they will just have spent more money on the system. That is based on what I said earlier. If there was an operational case, Danish law enforcement should have been able to prove it for the customers that were not affected by the suspicions.

Shabana Mahmood: How would you say this potential second version in Denmark compares to the proposal in our draft Bill? Is it a similar range of powers this time and similar coverage? Will it be less or more, do you think?

Jesper Lund: It will probably bring it closer to what is proposed in this Bill. I have been in contact with the Danish telecommunications industry and it has had fairly limited discussions with the Danish Ministry of Justice about this. There has been a single meeting in 2015. I do not know whether the Ministry of Justice is going to propose this to Parliament. It could happen this year or next year. The Ministry usually consults the telecommunications industry to a greater extent before it does something like this.

Q244 Matt Warman: Mr Binney, we have heard repeatedly from various different agencies that they would always rather be targeted and spend the resources that you have described, which are much smaller, doing one very targeted thing, but that they want to have the option

of having the haystack, as you put it, because that is the only way they can get to the people they need to get to in order to keep us safe. Your argument seems to be that they should be targeted, which they agree with you on, but that they should not have the option of the haystack. Can you explain how that would help?

William E Binney: The point is that they are interested in doing what they call target development, which is finding new people who are involved in that activity, whatever it is, whether it is dope or any other criminal activity – terrorism or so on. The point of doing the social networking reconstruction is that you can see those who are associated but not yet known. You can use other rules and smart things to do with software to look at the data to make assessments, such as the geolocation of positions and different things as they are passing by, and make a decision at that point about whether you want it. You can also put in other things. For example, you could classify as a target set all the known sites advocating jihad or any other kind of site you want, and look at who visits that site and how frequently they visit. That could put them in the zone of suspicion. That is how you do target development. That is really what they are after. You can do that in a targeted way with those kinds of rules added to it.

Matt Warman: That seems to be precisely what has been described to us. The ambition is not to have an infinite army of analysts but to have access to the pipe in order to target more effectively.

William E Binney: That is exactly what I am advocating, but you can do that upfront. You can make those decisions upfront, filter out all the other material, let it pass by and not even take it in. That gives privacy to everybody in the world and gets you the target set you want.

Matt Warman: Are you familiar with the request filter, as described in the Bill?

William E Binney: Yes, I think I am, but it is not the total Bill. You are still advocating bulk acquisition, and I am advocating stopping bulk acquisition.

Matt Warman: But, very briefly, it seems to me that the request filter filters out the bulk data. It does exactly what you are asking it to do. Are you saying that you do not understand that that is what the request filter does, or that you are not familiar with the details of how the request filter will work?

William E Binney: What I am getting at is that the bulk data is still stored and accessible.

Matt Warman: But not to the Government, thanks to the request filter.

William E Binney: You mean at the ISPs? The Committee needs to understand that there are many different things going on here that add to this bulk acquisition. It is not just the ISPs. If you look at some of the material that was exposed by Snowden, it shows clearly an upstream programme—the PRISM programme—looking at the ISPs contributing data upon request using a filter. The upstream programme captures everything directly off the fibres as it passes by. That is the bulk data acquisition that is available to GCHQ through NSA and all the other resources that contribute to that.

Matt Warman: But that is not what is in this Bill and not what we are talking about today. PRISM is fundamentally different. This is not a Bill that proposes PRISM.

William E Binney: No, but PRISM is an analogy to filtering because it filters too.

Q245 Lord Strasburger: The common factor between just about every successful terrorist attack in Europe over the past 10 or 15 years has been that one or more of the perpetrators was known in advance. Are you saying that attacks such as 9/11 and 7/7 could have been stopped if the agencies had used smart collection instead of grabbing absolutely every bit of data that went by?

William E Binney: Yes. In fact, in the case of 9/11, Tom Drake, who took over the efforts that I started with Ed Loomis to do a targeted approach, took the program and ran it against the entire NSA database in February 2002, very shortly after the attack, with the knowledge that we had prior to 9/11 incorporated in it. That program pulled out all the data that was in the database that NSA did not know it had on the terrorists prior to 9/11, so it gave them all the alerts, all the phone calls to the Yemen facility, all the phone calls back to Hamburg and to Afghanistan, even all the internal relationships, and showed all the data about who was involved in the attack prior to the attack. That would have alerted them. The difference was that we were putting in automated algorithms so that when they hit something of interest and we knew it was of interest, the program automatically executed. There were no people involved in that decision. So the program would alert everybody electronically and pass reports to everybody who needed to know once something was detected. It was done in an automated software way. We did not have the impediment of having people look into databases to find what was important in the data and so on. That would have at least alerted people and given them the opportunity to stop 9/11. The same is true with all the other attacks because all these people were known and in knowledge bases already. If the agencies had done a targeted approach from the beginning and kept the data finite, their analysts could have found the threats. That is my point.

Q246 Stuart C McDonald: Turning again to internet connection records, we have heard Mr Lund's views about their practical utility. Mr Binney, if this Bill is passed, can you see internet connection records being of practical use to law enforcement and to security and intelligence services?

William E Binney: Not in the bulk collection way, no, because again you have the same problem: if you take in hundreds of millions of records, you have to have people looking through hundreds of millions of records to find what is important. That is why the White House issued the Big Data Initiative in early 2012, soliciting corporations to come up with algorithms that would find information in big data that was important to look at. They issued that initiative because they have this problem, too.

Stuart C McDonald: I can see that from a security intelligence point of view, but I turn to a law enforcement point of view. One example that law enforcement gives us is missing persons. They say that because telephone records are pretty hopeless, they would love to have access to a missing person's internet connection records to see whom they have been communicating with. There are cases where they could have tracked a missing person more quickly if they had had the ability to do that. Do you recognise that as something that could be helpful?

William E Binney: Yes, and they can do that in a warranted, targeted approach. ISPs keep data for a short period of time afterwards, so it is still available.

Stuart C McDonald: What sorts of periods of time are we talking about?

William E Binney: I think that for most of them the figure with regard to their records is up to six months.

Stuart C McDonald: But do they do that? Is it a matter of practice?

William E Binney: Yes. On the web there is a list of companies' policies showing which ones keep data and for how long.

Stuart C McDonald: But at the end of the day you are accepting that there would be some practical utility in requiring the retention of records for six months.

William E Binney: Going after it in a targeted way, yes.

Stuart C McDonald: What do you mean by a targeted way, then?

William E Binney: Because you have at least the device that the person was using to connect with the internet, along with their phones and cell phones, so you have that data. You can use that data to go after them and data that was related to them.

Stuart C McDonald: Sure, but you would have to have retained en masse, because obviously you never know who is going to go missing, and then you have to go back.

William E Binney: The telephone companies keep that data for a period of time also, so you have that from them. You also have it from the ISPs for a period of time.

Stuart C McDonald: Okay. To both of you: what about the privacy implications of keeping internet connection records in the way proposed by the Bill?

William E Binney: To me, right upfront it destroys privacy. To return to the bulk issue, taking so much of it in destroys your capacity and makes your analysts dysfunctional. It makes your law enforcement people dysfunctional, too. They cannot find the data that is important.

Jesper Lund: In terms of privacy, you would basically be storing the entire internet activity of every British citizen, which is really intrusive. In the specific case of finding a missing person, what would be most effective would be if their mobile phone was still active; then the mobile telephone company can triangulate that phone using its mobile phone towers. If the phone is no longer active, presumably that is where a case could possibly be made for accessing internet connection records. However, those records may show you internet communications but they are not able to distinguish between active communications and the background communications that would happen on a smartphone at any time, even if it was left alone in a different part of the country.

The Chairman: I remind the Committee that just before 4 pm I will have to call the Committee to order because of the vote in the Commons.

Q247 **Mr David Hanson:** Imagine for a moment that your objections are not listened to and there is a scheme in place under the Bill that operates as the Bill currently proposes. The Bill says that £247 million is available over a 10-year period for the running costs of the Bill. In your professional judgments, is that a feasible resource to meet the costs of the Bill as proposed?

Jesper Lund: If you want an ambitious system for collecting internet connection records, it will be more expensive than the Danish system. Extrapolating from the cost of the Danish system, taking into account the difference between the size of the UK and Denmark, the limited version that we implemented in Denmark would take up what is set aside for internet connection records, so I think it would be more expensive than £247 million.

William E Binney: I think that that might be a good estimate for the retention and storage of data. I am not sure that it would cover the cost of processing, interrogation and development of software to do all this and of managing the data once you have it, having analysts look at it, whether you need more analysts and so on. There are a whole set of costs that go with data acquisition.

Mr David Hanson: The costs are detailed in the Bill, but essentially the Government have currently allocated around £180 million for the costs of establishing the collection of bulk data. Is that reasonable for 70 million people over 10 years?

William E Binney: From my perspective, that should be reasonable.

Q248 **Mr David Hanson:** One final question. We have talked a lot about privacy. TripAdvisor, Facebook, Twitter, Hotels.com, Tesco, the Co-op and Spotify probably know as much about me as the Government do. Is that a problem, or is it just the Government you have a problem with?

William E Binney: I would say that all those companies cannot come and arrest you, charge you with crimes or retroactively do research on you. For example, if you take a position that the Government are not in favour of, you can become a target, as numbers of people have.

Mr David Hanson: I suppose my question is: is the bulk collection of data by all those private sector companies more or less objectionable than the bulk collection of data by the Government to stop terrorism, paedophilia, criminal activity, drug abuse and all the other activities? That is a conjectural point.

Jesper Lund: I understand the question. It is also one that has occurred to me several times in Denmark. The important difference is that you give consent to those companies to collect your data. You choose whether to use Facebook and you can refrain from using it if you do not have faith in its data collection practices. You cannot get out of internet collection records. They show your internet activity and they are going to be retained, whether you want that or not. As I understand the British system, not all communication service providers will sign up to this, but you will never know whether the information is retained—

Mr David Hanson: I suppose that that also presumes that I am bothered about that. If I am not committing a crime, am I bothered about the fact that they could access it if I did? I just pose that as a question.

Jesper Lund: Sure, but my take on this is that privacy is a fundamental right that applies to the individual citizen, just like freedom of expression. Whether or not you want to use that right is your choice, but the mandatory collection of something like internet connection records infringes your right to privacy.

Q249 **Dr Andrew Murrison:** It has been said that the UK intrudes upon the privacy of its citizens in a way that practically no other western state does. I am concerned that the UK should be an outlier, if that is true. Clearly the point of safety is being with the pack; indeed, in a legal sense it is probably important that it is. What is your assessment of where this Bill would place us in terms of countries with which we can reasonably be compared in terms of the acquisition of data and the surveillance and control of that acquisition by the state? Sorry, that is a very broad and overarching question, and this is a very complicated Bill and there are parts of it that will apply to a greater or lesser extent in other countries. As a broad-brush approach, though, where do you think it would place us?

William E Binney: I think it would place you equally with the US, because this is exactly what the US does. It does it under Executive Order 12333, which has no oversight whatsoever in the US.

Dr Andrew Murrison: No oversight at all?

William E Binney: None at all, by courts, Congress or anyone. It is all done by presidential order. The Fairview programme is the primary programme for the collection of data against US citizens, and it has 100 tap points right across the US, distributed with the population. It is distributed in that way because it gives them the ability to capture all that data about US citizens. That is a violation of our constitutional rights and we have been trying to challenge it in court. They have been fighting like blazes to keep this out of the courts because they know that what they are doing is unconstitutional.

Dr Andrew Murrison: Presumably, that is a work in progress.

Jesper Lund: It is always hard to do these comparisons, even within Europe because sometimes the European Union has similar laws. My understanding is that the UK is at the forefront of data collection about its citizens in Europe. France is also stepping up the surveillance of its citizens but is taking different routes in certain areas—for instance, by forcing communication service providers to do some form of metadata analysis of the communications that are going through their systems, not just the retention of those communications. You see different approaches in Europe but my short answer would be that the UK is at the forefront of data collection.

Dr Andrew Murrison: In terms of intrusiveness?

Jesper Lund: In terms of intrusive data collection, yes.

Dr Andrew Murrison: And what about oversight?

Jesper Lund: It is probably even more difficult to do cross-country comparisons of oversight. If I compare the UK and Denmark, I would say that you have more oversight in the UK but also more data collection.

The Chairman: It has been a fascinating session for all of us. Thank you both so much for coming along and answering a diverse range of questions, and a double thanks for travelling from abroad.

Rt Hon David Davis MP (QQ 174-185)

Evidence heard in public Questions 174-185

Oral Evidence

Taken before the Joint Committee

on Wednesday 16 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Lord Butler of Brockwell, Bishop of Chester, Lord Strasburger.

Witness: **Rt Hon David Davis MP**, gave evidence.

Q174 The Chairman: Mr Davis, Baroness Jones, we are very grateful for your coming along to the Committee. We think that you have some very interesting things to say about this Bill, and I will kick off by asking a question that is so general you can make a general statement before individual questions. The same question, first, perhaps to Mr Davis and then to Baroness Jones: is this Bill necessary, and to what extent does it address your concerns, if it does so at all, about legislation in this area?

David Davis: Thank you for the welcome, Mr Chairman. It was either you or the Berlin Christmas market. You won this time, so I have just leapt off a plane. Is it necessary? Yes, it is necessary. There is no doubt that we need a new Bill. It is taking over, if you take David Anderson's count, something like 66 statutory mechanisms for various forms of interception, data gathering and so on, many of them based on bad laws. RIPA is a bad law. I am sure some of your witnesses have told you that already, but it is very badly drafted. I can come back to that in a minute. It is also taking over laws that are used in ways that I am quite sure Parliament did not intend.

I would have hoped that it would have consolidated all the electronic surveillance laws into one area. It has not done that, so its first failing is that it has not concluded that. You have just had witnesses from law enforcement agencies, have you not? The police Act is still effective. IMSI-catchers, the devices that block and intercept mobile phones, for example, would go around this, and that is part of the propensity to expand on the part of the agencies. All agencies in the world expand their powers, and this encourages it.

It is good for another reason and that is, in a consolidated form, that it will be possible not to future-proof it but to future-adapt it. A lot of the argument that you get from the agencies is that we have to make this future-proof, which tends to be an argument for making things more general, open and loose. That is a bad idea, but we are probably going to have to get into the habit of probably having one of these Acts every Parliament anyway—just as we have a Finance Act every year and a Companies Act every year or two—because of the rate of change of technology.

Does it meet all my concerns? You would be surprised if I said yes, would you not? The answer is no. On authorisation, which again I am sure we will come back to, it is a missed opportunity, because a new consensus was developing on judicial authorisation. They have missed that. It is certainly not what somebody described as world-leading. If I had to pick the world-leading country in this area, I would probably pick the United States for where it is arriving at now rather than us. I do not think that the double lock is very good. It claims to introduce one new power, but in practice you have internet connection records as well as effective recognition or avowal of bulk equipment interference, bulk personal data sets, bulk data and even thematic warrants. Although they were not formally approved by Parliament, somehow they were invented out of RIPA. There are a whole series of areas where it is weak, but broadly speaking we have to have a Bill along these lines.

The Chairman: Baroness Jones, if I can just repeat the question, is the Bill necessary, and to what extent does it address any concerns you might have about legislation in this area?

Baroness Jones of Moulsecoomb: Lord Chairman, thank you very much. I am missing our team Christmas do and they are all in the pub waiting for me, so I am sure you will understand if I speak quickly. I suppose you could say it is necessary, because times are moving on. Obviously we now have huge ability in surveillance, and so some sort of way of containing it and monitoring it is incredibly important. The majority of powers in here are new.

My concern is twofold. First, this is covering what has been done up to now, because the laws that have existed so far have been broken and abused many times by security agencies and by the Met. I have quite a list, which perhaps I could give you subsequently. I am concerned that there is a good operational case for this and that they really understand how to use the powers. I am concerned that they are going to use these powers to spy on people who are holding them to account, because this is what has happened already. Security agencies and the Met Police have used powers that they do not have to spy on people, for example Doreen Lawrence, who tried to hold the police to account. Mark Thomas, who is a comedian, tries to hold the state to account. There are five journalists who have been spied on so far, and even I had for 10 years, when I was an elected person sitting on a police authority, a file on me in the Met's domestic extremist database, which is fairly outrageous. I am quite clear; my life is quite public and there was nothing to hide, so I do not feel that I was intruded upon, but at the same time what a terrible waste of time and resources, and it was not just unnecessary but unlawful at that stage.

There is also the fact that Snowden has told us that GCHQ intercepts 50 billion internet communications a day. Now, that is an astonishing amount of data coming in. Over the years, I have asked the Met Police how many databases they have to get an idea of how much information is coming in. They could not tell me to the nearest hundred or to the nearest thousand how many databases they had, so we are looking at something that is potentially very complicated. There is a vast amount of information coming in. Do they have the skills to deal with it?

Q175 Suella Fernandes: I have one general question. Do you agree that the Bill before us today represents progress compared with the Draft Communications Data Bill in 2012?

Baroness Jones of Moulsecoomb: I would say that there are things in here that I am deeply unhappy about.

Suella Fernandes: How does that compare with what we last saw in 2012, in that now local authorities do not have any powers? That is a movement from 2012, is it not?

David Davis: There are marginal improvements. There is no doubt about that. As I said, the fact that there is a single Bill of itself is an improvement, but it is a long way short of what it should be. One of the things that worries me, Chairman, and I hope you will take this in the spirit it is intended, is that it is going to be incredibly difficult for you as a Committee to deal with this Bill in the time available. It is an enormous Bill, particularly when you take on board all the newly avowed powers. They are not new powers in the sense of being used, but they are new for Parliament. Assessing whether they are right or wrong, effective or ineffective and proportionate or not an erosion of privacy is going to be incredibly difficult, and in this business speed is the enemy of wisdom, so it is quite difficult.

My comment is that they are granny footsteps towards a better position. We must not miss the opportunity to get this right, both from the point of view of protecting the values that we are supposed to protect and, on the other hand, making the agencies more effective. They are behaving in a very different way from some of our allies, who are arguably more effective.

Baroness Jones of Moulsecoomb: The Government appeared to make some concessions, because there was quite a furore about this. For example, they brought in judicial review, but the judicial review is very light and in fact can be completely ignored. If Ministers decide there is some sense of urgency, they can go around the judges altogether, despite the fact that the Royal Courts of Justice has a judge on duty 24 hours a day. They appeared as concessions but they do not go far enough.

Q176 Lord Butler of Brockwell: If I may follow up that point, when you say that the Government could ignore the judges completely, are you referring to it being within five days if it is a matter of urgency?

Baroness Jones of Moulsecoomb: Yes.

Lord Butler of Brockwell: If I may respectfully say so, surely that is not ignoring the judges completely.

Baroness Jones of Moulsecoomb: They can bypass them.

Lord Butler of Brockwell: It is for five days.

Baroness Jones of Moulsecoomb: Perhaps I can talk about the volume of stuff that is coming in. The Prime Minister will be told if there is a warrant for people like us, for example—privileged people. For me, those are the people we are going to have to be very concerned about. These are the people who get whistleblowers coming to them, whether journalists, ministers of religion, parliamentarians or whoever. The Prime Minister will be notified of a warrant but does not necessarily have the right to reject that. The warrant will go to a judge. Am I saying this wrong? The judge or the commissioner only reviews it. The judge is not able to say yes or no. The Minister can then take it to the investigatory powers

commissioner, who can overrule the initial commissioner, so there are lots of ways in which these things can be pushed through.

Lord Butler of Brockwell: I will not continue this, but the investigatory powers commissioner is of course a judge.

Baroness Jones of Moulsecoomb: Yes.

David Davis: Lord Butler, can I give you my view of this, which is not the same? I do not view the accelerated procedure as a necessary bypass. It is going to have to be refined in some ways, but of course there are circumstances in which fast decisions have to be made. In the London/Glasgow bombings, for example, telephone data was very important and you had to make a decision very quickly indeed—maybe in minutes. You have to have a procedure like that. There is of course, in my view, a need to keep a very close eye on it and maybe publish how many times that is triggered every year. Frankly, make it plain to an officer who uses that procedure that if he is in the wrong there will be a mandatory warning on his record, but I do not see it as a bypass. I do not share that concern.

Q177 Lord Butler of Brockwell: Thank you very much. Could I get on to bulk interception? Are you satisfied, and I may ask each of you in turn, that the operational case has been made for bulk interception, bulk acquisition of the collection of communications data and bulk equipment interference? Perhaps I could use my second bit of ammunition before I ask you this question. This is a matter that David Anderson looked at and said he was satisfied that those powers were necessary. Do you agree with him?

David Davis: I do not entirely. Let us take bulk interception first. It is insufficiently narrowly defined for foreign for example. Charles Farr, when he gave evidence in 2012, I think, said that the selectors on the bulk intercept data would obviously pick up British-to-foreign intercepts and would treat accessing Facebook, Twitter or any foreign platform as appropriate for this. That seems to me to be too broad and that they have not made the case to justify it being that broad. If we are talking about bulk intercept of a fibre optic going through Cyprus to Pakistan, I am going to be more relaxed about it. That is the first thing.

Your second point was about the bulk acquisition of communications data. The best model here is America's. They basically recoiled from that after the President's panel had a really deep look at it. There was a previous director of national intelligence and very serious counterterrorism lawyers on the panel. They looked at it and came to the conclusion that what they were doing was simply not worth it. We would have to make a much stronger case to come back on that.

On bulk equipment interference, individual targeted equipment interference is obviously a necessity, particularly in this day of encryption. It is one way of getting around encryption and probably the most effective, but bulk interference worries me a lot. It is a very serious intrusion of everybody's privacy. We know already that one of the agencies has effectively suborned very large numbers of SIM cards—in the millions. That sort of thing worries me. Apart from the direct assault on individuals' privacy by the state, it would undermine the integrity of their own personal security to anybody else—to a blackmailer or to somebody trying to intercept them.

One group that you did not mention which I am going to raise because it almost falls off the tongue is bulk personal data sets. It is avowed, but there is very little in here. It is not for me to give the Committee advice, but if I was going to point at something that needs to be looked at, I would look very hard at that as well. This has explicitly been disavowed as an approach by the Americans and others, and it really is completely antagonistic to the things that the current Government and the previous Government set their face against. In the identity card arguments, the primary argument about the identity card was not about carrying a plastic card but about the existence of a central national database of personal data on every citizen, and it sounds to me as though we have had that since certainly 2005 and possibly 2001, which is what shocked Mr Clegg. There is a very large number of areas where other people have found that these are very bad ideas and do not work and have recoiled from them, sometimes even the agencies without external intervention, on cost-effectiveness grounds. We need to have a much tougher, more challenging attack on this if we are going to justify it.

Lord Butler of Brockwell: Just on that last point about bulk personal data, are you reassured by the fact that under the Bill this would now require a warrant that would have to be endorsed by a judge?

David Davis: That is an improvement, but on the very holding of this, I do not know whether you can see the data sets that they have. We are pretty sure, at least reporting on the register today, that they have all the communications data. They have flight data. They almost certainly gave financial data. They may well have ANPR data. This is very intrusive information for a state to hold. We have been having arguments for the last 10 years about whether we should have a central database for ID cards, or whether we should have communications data, hence the stalling of the so-called snooper's charter, when in fact this has existed throughout that. One thing that I would hope the Committee would come to a view on is what is in this, because there are arguments that there are hundreds of data sets here per person, which is really very serious. Yes, you are right that warranting is good, but frankly the extent to which much of this database should exist is very debateable.

Baroness Jones of Moulsecoomb: There are also, of course, medical records and financial asset records, and so on, in those data sets. It is a very wide scope.

Lord Butler of Brockwell: Baroness Jones, do you want to add anything on bulk collection?

Baroness Jones of Moulsecoomb: The bulk collection of domestic phone records, of course, has been proved to be ineffective in the States under a similar power. The President's review group said that it was not essential to preventing attacks. The Privacy and Civil Liberties Oversight Board concluded that it had not identified a single instance involving a threat to the United States from that sort of collection, so I would argue that it is of very limited value.

Q178 Victoria Atkins: Just on that point, you have listed all sorts of information. What is the basis for asserting that those are sets of information held by the authorities? How do you know? You have told us that with some confidence.

David Davis: Some of it has been around. The place to look is an organisation that used to be called GTAC—probably in your day, Chairman. It is now NTAC, the National Technical

Assistance Centre, based at Thames House. It has already been recognised in public by Ministers that intercept data is there. These are the people who handle most of the requests from all the agencies. It has been in the public domain that there is a financial set, which I assume is credit cards and bank records, because GCHQ has a title for it: FININT. Flights we know about. The question was about the rest. As to whether or not they have ANPR, it would be very surprising if they have this and have not put ANPR in it, for example. If I were going to build a database like this, given their purpose, that is what I would do. It needs to be answered. One of the things that has been said for a start by a number of security journalists, who know their way around this, is that they think there are hundreds of data sets—not one, not five.

Victoria Atkins: Do you worry, in listing these data sets as you just have, that you have given some very helpful information to serious organised crime gangs, terrorists and others?

David Davis: In that case, I would arrest Malcolm Rifkind, because he drew it to the public record in March last year. It was only when that was done that this was put under the intelligence commissioner's oversight. Until then, there was no oversight whatever. I am afraid that in a democracy it is necessary to look at what you are doing, and you can only do that by discussing it.

Baroness Jones of Moulsecoomb: The scope very definitely has to be well defined, which it is not at the moment. There is also the fact that once you have warrants for this bulk information, access is much freer. Once you have it, there are stacks of stuff in there that you can freely search whenever you have an appropriate moment. It is not just a one-off search.

Victoria Atkins: I have a question to both of you: what is the correct balance between the democratic accountability of Ministers and the independent oversight of judges in the authorisation of warrants? Does the draft Bill get this right?

Baroness Jones of Moulsecoomb: I would like to have seen a little more of the judges being able to look at the legal aspects of whether or not to grant a warrant. That is lacking at the moment. Politicians vary enormously in their skills and may not be the best people to have that sort of last word or ruling.

David Davis: Our approach to this and that of some of the Commonwealth countries is based on the royal prerogative concept of government. That it adds accountability I would dispute absolutely. Jack Straw always used to say that when you are in trouble, the safest place to be is the Dispatch Box of the House of Commons. That is certainly true when it is a terrorist event. I was the opposition spokesman who responded to Charles Clarke on the day of the 7/7 attack, and you can be quite sure that the aim of the Opposition at that point was not to embarrass the Government; it was to show solidarity against an outsider. That always happens. You may remember Gibraltar, when the Labour Party was very supportive. Even though there were some doubts on the day, they were very supportive. Even a few weeks ago when we had the drone attack, there were some differences between the Prime Minister's approach in the Chamber and what was written to the United Nations, but nobody went for that, because we and the public take a view on this.

Secondly, when it comes to warrants, it is very often illegal for the Minister to talk about it publicly anyway. I suspect that you have had some Ministers in on this. It is legally forbidden to talk about it. The pressure on a Minister to be accountable is near zero. If you look in *Hansard*, you will find a number of Parliamentary Questions from me asking the mundane question: what law, what statute, was this done under? I got the answer that we never comment on security matters, so we do not even know. That is how accountable it is; we do not even get an answer about which statute is being used.

First, the accountability argument is a chimera. It is a problem for countries such as the States, which takes a very different view of the royal prerogative than we do, obviously given their foundation. Many of them view the idea of ministerial approval as being rather flawed.

To take up the Baroness's point about skill, we are very unusual at the moment. We have a competent Home Secretary who has been there for over five years. When I was shadow Home Secretary for five years, I had four opponents, one after another—Blunkett, Clarke, Reid and Smith. The typical tenure of a Home Secretary is about two and a half years: a year getting into the job, a year understanding it, and then they are on their way. What do they do? What does this warrantry process consist of? There were 2,345 warrants last year: 2,700-odd in total, but 2,345 signed by the Home Secretary. That is about nine a day on a working day, if you assume that she signs one or two before going to church in a hurry on Sunday. It is about nine a day on working days, 50 weeks a year. That is not long enough to do this. Fifteen or 20 years ago, there were about 1,000 a year. I spoke to one of the Home Secretaries who did it then. He said that even 1,000 a year was too many. You never got enough information to make a judgment; you got a précis of the case. You cannot make a judgment on something as intrusive as this on a précis. You get no chance to do much cross-questioning.

Victoria Atkins: Which Home Secretary is this?

David Davis: You will have to call him yourself.

Victoria Atkins: I cannot if you have not told me.

David Davis: I am not going to tell you without his permission.

Victoria Atkins: This is hearsay.

David Davis: No, I am just telling you. You can work it out if you try a little. One thousand a year is what they did then. It is now at 2,500 and going up. From that point of view, compare that against using a judge or a panel of judges. First, they are more expert. They are in the job for a long time. Look at the example of SIAC. If we were smart about it, we could do what the Americans do and effectively put up a special advocate to challenge and make sure that the public interest is maintained. That is the way to do it. That is much more effective than this way. I am afraid that this way will improve it slightly, but it misses the optimum outcome.

Victoria Atkins: A simple question: who judges the judges?

David Davis: We are going to have a whole new procedure in place of other judges. Most judicial systems have a structure to them where things are reviewed further up. That is what has happened here. That putting-together of the overarching commissioners, by the way, is a very good bit of the Bill. That is straight out of Anderson, and Anderson was exactly right.

Baroness Jones of Moulsecoomb: What we are talking about here is high-level authorisation. I heard the police officers talking earlier about who was going to be able to give such authorisations, and it can in fact be at a much lower level. A detective sergeant was found last year giving out authorisations.

Victoria Atkins: Was that of intercept warrants?

Baroness Jones of Moulsecoomb: Yes.

Victoria Atkins: That is not my understanding.

Baroness Jones of Moulsecoomb: No, but it is an indication of where a structure can break down, because that detective sergeant did not even know that journalists had a duty and a right to protect their sources. Things can decay in use, which is my experience of the Met Police.

Victoria Atkins: Is the proposed procedure for urgent applications for warrants for intercept, part 1 of RIPA, appropriate?

David Davis: We have different views on this, as is apparent from the answer to Lord Butler earlier. I think it is broadly appropriate. Five days is quite a long time, even in the Civil Service, so it could be shorter than that, but as I said we should publish the number of times we use these every year. We should establish some clear criteria. Obviously in an imminent life and death situation it is a no-brainer, but there are a few others that may not be quite so clear-cut. The London/Glasgow bombing is one example. It was not imminent life or death; it was 12 hours or whatever it was before the attack, but those hours were slipping away. They needed to move quickly with what information they had, and it is very hard to legislate for that, so you have to allow a little tolerance in the urgency. There may also be some circumstances in which there is the possibility of losing information. Information is only available for a very short period. Just those three completely different criteria demonstrate that urgency is rather hard to define. It is very easy to recognise and hard to define, but we could certainly write a statute to cover that.

The Chairman: What you are saying, Mr Davis, is that with regard to the urgency, in your previous answer to Lord Butler, you would advocate first of all that the time of five days is shortened and, secondly, that there might be some special investigatory process for those urgent ones to ensure that they have been dealt with properly, as urgent.

David Davis: That is right. The other thing that I did not mention, of course, is that under my preferred approach, which is a permanent on-duty judge, you are going to have less of a problem most of the time, unless we are happy to wake up the Home Secretary every moment of the day and night. You would have a 24-hour panel. You would still need a process, but it is the sort of thing that I would only expect to be used relatively few times a year—single to double figures, no more than that.

Suella Fernandes: Just to follow up on this, have either of you ever authorised any warrants?

David Davis: I have refused to authorise one.

Suella Fernandes: Is that to be read that you have not been involved directly with any authorisation of warrants in your roles?

David Davis: Yes, except for the one occasion.

Q179 Stuart C McDonald: You have both made pretty clear your views on having this double lock of first a politician and then a judge, but assuming that we retain that double lock, what standard of review is appropriate?

David Davis: This has been quite an area of argument, of course, because the Bill states judicial review standards. Of course, that leads you down all sorts of routes. If you take Wednesbury standards, which is a sort of procedural, "the Minister must have been out of his head", clearly that is not good enough, as often as that may happen. The real standard, and why I wonder why they put in judicial review standards, is that basically it should be a judgment about necessity and proportionality. That is what should be there. There have been debates. Have you had David Pannick in front of you?

The Chairman: No, we have not.

David Davis: You have had people quoting him, I am sure. He says that in these cases it is not really Wednesbury; it really is proportionate when it involves human rights. He was citing cases where people's liberty was at risk, basically in SIAC and so on, which is quite serious. In the very next paragraph of his article, he talks about how judges do not like to overrule the Executive, the Ministers, particularly when it is a matter of national security. You have a balance both ways. One of the things that this Bill needs is absolutely explicit explanation of how the judge will make the decision so that there is no doubt about it. I also think there is a problem about the judge going immediately after the Home Secretary. It is a pretty brave judge who turns over a Home Secretary.

Baroness Jones of Moulsecoomb: I feel more or less the same way.

Stuart C McDonald: The two former Secretaries of State who we had before us were both horrified at the notion that you would have detailed or intensive scrutiny of decisions involving things like life and death, but you seem to be the opposite way round: these are the ones that would require a higher standard of scrutiny from judges.

David Davis: Can you say that again? What did they say to you?

Stuart C McDonald: They seemed to be aghast at any sort of notion that a judge would engage in a very strict and detailed scrutiny of decisions on imminent matters of life and death, for example.

Baroness Jones of Moulsecoomb: Judges are trained to assess evidence and to assess whether or not a course of action is appropriate. I would argue that that surely is a better route.

Stuart C McDonald: You would essentially want the judge to make a decision fresh themselves, based on the same evidence. It is as simple as that.

David Davis: If you really had to have a double lock, which is a silly title for it—it is more like a loose latchkey—I would put the judge first.

Q180 Suella Fernandes: You have mentioned David Pannick's article, but we have heard evidence from Lord Judge, who is the former Lord Chief Justice and head of the judiciary, and Sir Stanley Burnton, who is the Interception of Communications Commissioner. They both, as senior judges, have experience in this area of law. They have both said that the judicial review test here necessarily imports the test of necessity and proportionality, and that it is the right test that strikes the right balance. Are you disagreeing with them?

David Davis: Yes, I am. Let me give you an example of why, from the intelligence area but not from intercept. In the case of Binyam Mohamed, when the Court of Appeal was considering whether or not to put into the public domain a five-line summary—nothing harder than that—of the fact that the British state had likely been colluding in torture, it took them months to get round to doing it because they were so reticent about overturning the opinion of a Foreign Secretary. They did it eventually only when an American court published the hard data. Even then, they redacted from their own judgment comments about the agencies. Now, that is a very good parable, but it is not the only one of judges being very cautious, and you can understand why, about critiquing an existing government decision, an existing Secretary of State's decision, particularly quickly and particularly with national security. They are just as susceptible. They are not saints. Judges are as variable as Ministers in some respects, but they are human. They do not want to be the person who says, "No, you cannot do that", and then somebody gets killed. After all, at the end of the day, that is the core question in all this.

Suella Fernandes: Do you not think that, for transparency purposes, if there is a threat of an imminent attack, for accountability, legitimacy and reassurance for the public it is the Home Secretary, a Minister, who will need to face members of the public on making a decision, not a judge behind closed doors.

David Davis: The Americans do not find that.

Suella Fernandes: We are not America.

David Davis: No, I am giving you an example of where it does not happen. The Americans do not find that. Nor have I seen a single example in my time in the House of a Minister being held to account for a failure of the services—just the reverse. Go back and look at 7/7. The Opposition very carefully, some may remember, did not call for an inquiry into that. Why? The actions of the political body, in toto, were to act in solidarity, not to challenge each other at that point. The accountability argument does not stand up. I do not think that the public are even aware, most of the time, of individual warrantry.

Also, we are talking about terrorism. Let us be clear about this, because I may have a different view from other members of this Committee: terrorism is not a war, it is a crime. By calling it a war, we give advantage to the other side. It is a crime. We do not require Ministers to sign off warrants on other crimes. I do not see why the public would necessarily

expect them to sign them off on this. What the public wants is a safer outcome with the minimum of intrusion into their lives. They will not be worried about the procedure.

Baroness Jones of Moulsecoomb: There is also the fact that it is very hard for any Home Secretary or any Minister to say no to the security services, if they are saying, "You must do it. You have no choice". I would have thought it would be far better to rely on a judge having looked at the evidence and assessed it properly.

David Davis: I do not necessarily agree with that, to be honest. The current Home Secretary does say no to some.

Baroness Jones of Moulsecoomb: I would agree that Theresa May is doing a splendid job.

David Davis: That was not the point that I was making. She does say no to some. The one I am unwilling to name, but I will ask if he wants to name himself, certainly said no to some, more than some, so I do think that they take it seriously, but I just think that they are making a decision on a précis. This is a life-changing decision, and it is sometimes a life-saving decision, on the basis of a précis.

Baroness Jones of Moulsecoomb: I did not say they would not. I just said it is hard.

Victoria Atkins: Mr Davis, you said that it would be a brave judge who stood up to the Home Secretary. Does that not undermine your argument that judges should be solely responsible for this process, because if they are not brave enough to stand up to the Home Secretary, the Foreign Secretary or the Northern Ireland Secretary, one wonders how much they are adding to the whole process?

David Davis: They are good and poor procedures and this, in my view, is a poor procedure. That is the point. What pressures are built into the procedure? You design judicial procedures to give a fair outcome, and you should design these procedures to give the best outcome, the optimum judgment, from the judge, and this is not the way to do it.

Q181 Lord Strasburger: I have a slight change of tack. Some jurisdictions have a method for informing those who have been subject to surveillance after the event, after the case has concluded, thereby giving them an opportunity to seek redress, perhaps in our case through the IPT or perhaps through normal courts. Do you have a view on that?

David Davis: Yes. In the countries that do that, it is quite constrained. Obviously if somebody is still subject to investigation, it is never going to happen. If there is an ongoing case still, it is never going to happen, and even if it is the next-door neighbour it is not going to happen. Nevertheless, the existence of such a procedure is a very good discipline on the agencies themselves and on the people making the decisions, because that way mistakes will out eventually. Frankly out of all of them, only a relatively small number are ever declared, but the existence of the procedure is quite good.

Q182 Shabana Mahmood: I just wanted to return to this whole politicians against judges argument. Is the whole point not about political accountability—the "who judges the judges" question? The politician in this scenario is trying to achieve something different, which is a unique threat, a unique capacity for scale of death and slaughter, and making a decision very quickly. The judges are fundamentally doing something very different, which their training

teaches them to do. It is fundamentally different from the politician's job. Why do you think that political accountability should go from a process that is only about judges simply applying the letter of the law, making a judgment on the day, but not worrying about any other of the ramifications that that might have for our national security?

David Davis: I think I have said twice now, so forgive me, Chairman, if I am repeating myself for the third time, that the operation of the House of Commons in particular, in terms of effecting accountability, and indeed the operation of the British media, because the British media also go shoulder to shoulder when this sort of attack happens, is not one that delivers conventional accountability. Let us imagine for a second that we had a Spanish situation. One reason why, when I was shadow Home Secretary, the Conservative Party redesigned our approach to what we would do in the event of a terrorist attack was because of what happened in Spain. As it happened at the general election in Spain, I thought it might happen at the general election in Britain, so I thought, "This is not going to happen in Britain".

Let us imagine for a second that it did and that we tore into the Home Secretary of the day because the agency had fallen down on this, that and the other. The truth of the matter is that they did fall down on some things. I am not going to replicate them here, but they are easy to look up. The last thing we would be worried about is who signed off the warrant. It would be what did not work. What did not work? We know what did not work. They had information about Mohammad Sidique Khan. They had a photograph, and they cut it the wrong way and sent it around in an unrecognisable form. This procedure does not add to the accountability. It seriously undermines the effectiveness of the process.

Shabana Mahmood: Your argument is a very compelling takedown of the political class being a bit rubbish, which we may or may not agree with. You have a point about accountability, but is that not a better argument for improving political accountability in the system, making us work harder in the Commons and making us work harder as an opposition, rather than saying politicians are rubbish, so let us just hand it over to the judges, who apply a whole different set of principles?

Baroness Jones of Moulsecoomb: I am not saying that politicians are rubbish. I am saying that they are only as good as the information they are given. Quite honestly, having watched the Met over the past 16 years, I know that they can be extremely selective about the information that they give you. That may not be true for the security services; I do not know, but I think it likely is.

Shabana Mahmood: If we accept rubbish information, we are failing to do our political job. I still have not heard an argument that says that we should move away from the realm of political accountability to legal accountability.

Baroness Jones of Moulsecoomb: We do not know it is rubbish.

David Davis: That is to misrepresent the argument. The second legal issue here is that I think you will find that for most of these warrants they are forbidden to tell anybody, even the House of Commons. Again, go back and look. I have not read that piece of the Bill—the 299 pages. I cannot remember what it said on it anyway, but most of the time these warrants are incapable of being put in the public domain. You have a problem there too.

Accountability does not work at this level, and you have to ask yourself at the end of the day what you are trying to do. You are trying to have a counterterrorism policy that works and is very effective against terrorism, and works as well as you can make it in relation to the protection of privacy. Those are the two things. We are trying to find an optimum in that. Nobody says that either side has an absolute, I hope, but we are trying to find an optimum in that. The optimum seems to me to be much better with a fully trained judge, with lots of time, with a full case, at any time of night or day, because you will have a panel of them, possibly with a special advocate to argue the counter case. That is guaranteed to make a better decision than a Minister.

Q183 Lord Strasburger: I have to say that the Bishop and I are the only people here on the panel who are not politicians. Some people have suggested that a way out of this conundrum is to keep the Secretary of State involvement in cases of national security and leave it to the judges for the rest. Would that open it up for you?

David Davis: The ISC set one level. I think it was just taking crime out of it. RUSI set it a bit higher, at national security; and Anderson set it a little higher still, effectively at defence and foreign. Anderson had a good argument when it came down to what I think of as the Angela Merkel conundrum. If you are going to bug a foreign Head of State, and I am sure we do not do that, there are political consequences. There are diplomatic consequences to almost any foreign operation. I would have a rather different approach. In fact, the approach in the Bill is okay for foreign operations, so I would draw it somewhere there. I have forgotten who said it now, forgive my poor memory—too much German wine—but somebody said, "foreign and significant people in the UK". I do not accept that one. I think that would be a very bad idea, because you would get back into all the establishment stuff. Broadly speaking, I can see a very strong argument for foreign, but outside that, no.

Lord Strasburger: What about national security?

David Davis: National security is such a hard thing to define. If you are talking about terrorism, whatever the Prime Minister says we are no longer talking about an existential threat. This is not the Soviets or the Nazis. In those circumstances, you could see some sort of argument for clearly defined national security. National security is a very broad-based thing now, with a very small number of targets. I would be inclined to say that you would have to have a narrower definition of that for me to be sure.

Baroness Jones of Moulsecoomb: Perhaps I could note two problems with that concept. The first is that definitions are not defined clearly enough, whether we are talking about national security, operational purpose or whatever. The definitions are, at times, quite slack. The second thing is that intelligence is likely to be shared. There is no limit on sharing information with our allies, for example with the Five Eyes. That is a big problem. It is all very well to accumulate information on what we see as our own national security, but will it impact on others?

The Chairman: We move now to the non-political Bishop of Chester.

Q184 Bishop of Chester: I have been thinking that if we had had Owen Paterson and David Blunkett with the two of you, we would have needed a week for the meeting. Owen Paterson

gave an impassioned defence of accountability at the Dispatch Box as being the appropriate accountability in a democracy.

David Davis: Did he give an example?

Bishop of Chester: When we had Lord Judge, any suggestion to him that the judge would not be entirely independent and able to stand up to all comers was regarded as an offensive suggestion, not least from someone like me.

David Davis: Judges are all saints.

Bishop of Chester: This was what Lord Judge said. Given the architecture as we have it, how can we improve and turn the latchkey into a double lock, as it were? The judges are appointed by the Prime Minister, not the Judicial Appointments Commissioner. They are reappointed every three years. Is there a way of taking the architecture, flawed though it may be, and strengthening it, making the judicial thing stronger and more independent?

David Davis: You cannot make it the best in the world. You cannot make it world-leading, which is what is claimed for this. Mind you, Malcolm Rifkind claimed that the last system was world-leading too, so you cannot make it that. If you want to improve at the edges, then certainly have a judicial appointments panel appoint the relevant judges. It is a technical decision, not a political one. Certainly have longer tenures or maybe even single tenures. Judges I know are inhumanly strong, but they may unconsciously be affected by that.

One of the things in the Bill that I thought was a very bad idea was that in effect it looked as though the Home Secretary judge made a decision on the funding, and it should not be done that way. There should be a Barnett formula for security, where the fraction goes: if you increase the size of the intelligence budget or the secret budget, you give 0.1% or whatever it might be. Make it a formula. Alternatively, you should have a direct negotiation between the lead judge and the Treasury. You must not have the person being checked up on deciding on the funding. Lord Butler would recognise an NAO model, basically.

Q185 Matt Warman: Do you think that this Bill adequately enshrines the Wilson doctrine in statute?

David Davis: Lord Wilson died a long time ago and so did this policy, I think. The Wilson doctrine has always been a very tenuous policy. It is always down to, "If I do this, I will tell the House when I think it is appropriate". That is almost certainly not soon in most cases, by which time the individual Prime Minister has moved on. I would be amazed, to be frank with you, somewhat shocked even, if in the classifications no Member of Parliament had ever been intercepted. I can think of some good reasons over the decades, so I do not think it is quite what it is seen to be in the public domain. It is not a ban on intercepting MPs at all.

In fact, I would take this away from the Prime Minister altogether. I can see even less reason for a politician to judge on whether or not you should tap a politician's phone. If you think of the arguments we have had in the last few weeks, Jeremy Corbyn has been called a threat to national security. Now, I guess it was just hyperbole. Nevertheless, it introduces a question as to who should do this, so it seems to me there are different criteria—and by

the way, they are different from what is written in the Bill, too. The Bill says "MPs and their constituents". In a way, the MPs-to-constituents link is almost the least worrisome, because it is the least interesting to the agencies. MPs to whistleblowers, MPs to journalists, in fact MPs to anybody is what I would make that, and I would make that criterion high.

It is not just MPs, mind you; this is a general privileges issue. With journalists, of course, the Government jumped in and fixed straightaway. You can guess why. The group you are looking at is lawyers, MPs, doctors, clerics and journalists, and none of them should be completely immune. I say that, but again, Chairman, you may remember that at one point some of the terrorist groups in Northern Ireland used doctor's surgeries' receptionists as handoff points, so you cannot make anybody immune, but you have to have a significantly higher threshold, and it really has to be a judge who decides. That is how I would deal with it.

Baroness Jones of Moulsecoomb: I have asked the Met about this and they call us privileged people, those people who come into this group of having certain rights, duties and so on. They apparently do not have a list of us. Obviously that list would change all the time in any case, but they do not have a list, so it is down to the authorising person checking whether or not this person might be a privileged person and whether or not the Prime Minister should be told about the warrant. It is all very specious, I would say.

David Davis: Chairman, I have forgotten one point. One of the things that has become apparent in the last couple of years—it has always been true but has just become apparent—is that communications data is not subject to the Wilson doctrine. Now, communications data is much more important now than intercept, particularly if you are talking about whistleblowers. We have just changed the law in the last year or two, Chairman, to make MPs prescribed people, from the point of view of whistleblowers, and provide them with employment protection. If a whistleblower comes to an MP, he or she gets protection. This is important.

In the Damian Green case, you may remember that Damian Green's arrest was after a whistleblower in the Home Office was in contact with him. That is precisely the sort of thing you have to protect, so the Wilson doctrine has to apply not simply to intercept but to all categories covered in this Bill.

Matt Warman: As I understand it, you are suggesting that these privileged positions should, in particular, be solely a judge, rather than having two politicians, as is currently proposed in the Bill, rather than one.

David Davis: Yes, I would do that.

Baroness Jones of Moulsecoomb: Yes.

Matt Warman: You have said that you would extend that to journalists. Would you care to have a stab at defining a journalist in the modern age?

David Davis: No, I would not. I will leave that to parliamentary draftsmen. The most important group for me is lawyers. Let me tell the Committee why, because this is another of these areas where the Government have the threat back to front. The simple truth is

that when you were in the Cabinet, Chairman, the rule was that if a criminal was being intercepted and started talking to his lawyer, the tape was switched off and the intercept was ceased at that point. That was the rule, as it was understood by the Home Secretary in your day. That is no longer true. The IPT's inquiry into this metamorphosed into the data being recorded but kept in a flagged privileged way, and not shown to the prosecution counsel in any case. Now that is not true and the data is made available to the prosecution counsel.

Now, at some time or another, when one of these comes out, we are going to have a hardened terrorist released on to the streets because of the failure of equality of arms in British law. This is madness. How that metamorphosis happened, I do not know, but it has happened broadly in the last decade or two and it seems to me that we really have to fix that. This Bill has to fix that.

Baroness Jones of Moulsecoomb: This area is so incredibly complex. Lord Chairman, you asked at the very beginning if this Bill is even suitable. I would argue that circumstances have almost moved beyond the Bill at this stage. I took the liberty of sending some of you an encrypted email yesterday and, quite honestly, any criminal or any terrorist could do exactly the same. This Bill will not deal with that sort of thing.

The Chairman: That was a fascinating and a lively debate.

David Davis: It was better than the Berlin Christmas market.

Baroness Jones of Moulsecoomb: I am not sure if it is better than a Christmas party.

David Davis: Chairman, if there are a few issues you have not covered—and I know we are tight on time—can I write to you?

The Chairman: Of course. That applies to both you and Lady Jones. If there are things you would want to add to what you have told us this afternoon, you would be very welcome to do that.

David Davis: It has been a real pleasure, thank you.

The Chairman: Thank you very much indeed. We are grateful.

Foreign & Commonwealth Office (QQ 1-25)

Evidence heard in public Questions 1-25

Oral Evidence

Taken before the Joint Committee

on Monday 30 November 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Bishop of Chester, Lord Hart of Chilton, and Lord Strasburger.

Witness: **Lewis Neal**, Director, Intelligence Policy, Foreign and Commonwealth Office, gave evidence.

Q1 The Chairman: I apologise for the fact that we are two minutes late. Welcome to our witnesses. We have, of course, seen Mr Lincoln in another capacity. We have until between now and about 5.30 pm. As is normal with these arrangements, all members of the Committee will ask questions. I will kick off in a second, but I remind Members of the House of Lords that they should declare any interests when they ask the question. Perhaps I could ask the three of you a very general question to begin with. Could you give a few brief remarks on what the draft Bill proposes and why it is necessary?

Paul Lincoln: The draft Bill responds to the three reports that were commissioned in this area: the recommendations from the Independent Reviewer of Terrorism Legislation, David Anderson QC; the review that was done by the Royal United Services Institute at the behest of the then Deputy Prime Minister; and the report by the Intelligence and Security Committee of Parliament. All three reviews agreed that the powers associated with communications and the data associated with communications should be brought together in one place to make them more clear and transparent. This draft Bill attempts to do three things. First, it brings together, as requested, the powers already available to law enforcement in this area. It makes them clearer and more understandable than they have been in the past. Secondly, the draft Bill overhauls the oversight arrangements. In particular, you will have noticed that we have proposed a double-lock authorisation for the most intrusive powers, which consists of a Secretary of State authorisation as well as a judicial commissioner authorisation. Thirdly, the Bill ensures that the powers are fit for the digital age, so restoring capabilities that law enforcement would previously have had in relation to communications data by bringing in powers for internet connection records.

The Chairman: Thank you very much. I do not know whether your colleagues wish to make any additional points. If not, arising from that and to make it clear to the Committee, which of the proposed powers are brand new, and which of them are being rewritten in new legislation?

Paul Lincoln: This Bill is very much about transparency and oversight, which the three reviews all said needed to be improved, as this is about powers. The Bill brings the existing powers together. The only new capability that is provided for relates to internet connection records.

The Chairman: Yes, but what does that mean for oversight?

Paul Lincoln: It not only brings the double-lock system that I talked about for the most intrusive powers, involving Secretary of State and judicial commissioner authorisation, but it establishes a new Investigatory Powers Commissioner, bringing together the existing three commissioner bodies and providing additional resources and additional technical and legal expertise.

The Chairman: Thank you very much. Other than the expiry at the end of 2016 of the provisions of DRIPA, what would the impact be if we did not have this Bill?

Paul Lincoln: If we did not have this Bill, we would lose a once-in-a-generation opportunity to provide some of the additional oversight mechanisms that I talked about a moment ago. In terms of the powers and capabilities, a new capability is provided for that in effect restores powers that used to exist around internet connection records. We have provided data as part of the associated documentation with the Bill, which sets out the operational case for that.

Q2 **The Chairman**: Just one more question from me before I hand over to my colleagues. What has been the impact of the Digital Rights Ireland case and the Court of Appeal decision in the Davis case on the powers and the wording of the Bill before the Committee?

Paul Lincoln: The Government responded to the Digital Rights Ireland case by passing some fast-track legislation in 2014, the Data Retention and Investigatory Powers Act, which took account of the ruling on Digital Rights Ireland. However, on the back of that, a judicial review was brought against those powers, which Parliament had voted for. That judicial review, in the Divisional Court, found two reasons for which the powers were incompatible with European legislation. Since then, a Court of Appeal ruling has said provisionally that it did not think that Digital Rights Ireland set out a minimum set of standards for Governments to comply with, and on the back of that the Court of Appeal has remitted this to the court in the European Union. Therefore, we have considered that position and the powers and the associated processes for which Parliament voted in 2014.

Q3 **Lord Strasburger:** Could you tell us in which Acts there would still be surveillance, data acquisition or equipment interference powers after the passage of this Bill?

Paul Lincoln: We have taken the opportunity to bring those into this, when it comes to the primary purposes relating to accessing communications data or content, but the Police Act, for example, would still allow equipment interference for other purposes.

Lord Strasburger: Are those the only ones?

Paul Lincoln: Those would be a good example. Similarly, the Intelligence Services Act would allow that for the intelligence agencies.

Lord Strasburger: Will you be able to give us a list in writing?

Paul Lincoln: We can write to the Committee.

Lord Strasburger: Secondly, you indicated that all the powers except one already exist. I think that we need a bit more clarity on that, particularly about whether all the existing powers have been recently authorised by Parliament. Given that CNE was not avowed by the Government until February 2015, bulk interception was first mentioned in the ISC report in March 2015, and the collection of bulk communications data was not avowed until the Home Secretary did so this month, it would have been impossible for any of those, as well as several other powers in the Bill, to have been specifically debated and authorised by Parliament. Do you agree that it is high time that many of those existing powers were debated by this Committee and by Parliament?

Paul Lincoln: The powers exist already. As David Anderson said, this Bill is an opportunity to bring that more clearly into focus and to allow Parliament, as we take this forward, to take an explicit view on all the powers in the Bill.

Lord Strasburger: I think you missed my point, which was that the three powers that I mentioned and others have never been specifically debated in Parliament. Do you not think that it is time that Parliament did debate them?

Paul Lincoln: Parliament now has the opportunity to debate these powers as this Bill is passed.

Q4 Suella Fernandes: What is it about the character and scale of the threat that makes this legislation necessary?

Paul Lincoln: If people look at the products in the public domain, the Joint Terrorism Analysis Centre has independently set the level of threat to this country at severe, which means that an attack is highly likely. You have also heard that the Home Secretary, the Prime Minister and the intelligence agencies have said that seven plots against this country have been disrupted this year that otherwise would have ended up probably in some form of fatality. Equally, figures published worldwide indicate 12,000 terrorist attacks in 91 countries in 2013, the last year for which figures were publicly available.

Q5 Shabana Mahmood: How confident are you that the powers in the draft Bill are effectively future-proofed?

Paul Lincoln: By bringing the powers together we have looked at the question of future-proofing. The critical thing is internet connection records and restoring capabilities that law enforcement have traditionally had as part of that. Richard no doubt will talk later about some of the processes that we have been through in talking to communication service providers and other technology companies about the specifics of the technology.

The Chairman: Let us move now to Mr Hanson, who I know has a number of questions.

Q6 Mr David Hanson: As regards the old system versus the new system of judicial authorisation, I am interested in whether there is any likelihood of additional time pressures on decision-making.

Paul Lincoln: Each authorisation is currently considered on a case-by-case basis, and that takes a certain amount of time. There is no set time for looking at the authorisation. It

needs to be done on the merits and the complexity of the case. Additional time may be needed for physically having two people involved in that decision-making process. The system that was put in as part of the draft Bill allows for urgency procedures. If there is a time-critical situation, a judicial commissioner can sign off under that procedure up to five days afterwards.

Mr David Hanson: Could we expect that, for example, in the Christmas period, the new year period or Easter period? Is that feasible and doable? In an urgent circumstance, would that be acceptable?

Paul Lincoln: In urgent circumstances, we have systems now in place where we deal with Secretaries of State. We have rota systems in place and we can access Secretaries of State out of hours to work through those systems.

Mr David Hanson: In the event that the judicial commissioner disagrees with a recommendation from a Secretary of State, what is the mechanism for that to be examined? Is that it?

Paul Lincoln: If that happened, the judicial commissioner would have to set out in writing the reasons for that refusal. The Secretary of State can have a discussion with that judicial commissioner to work through the issues. For example, it might be that collateral intrusion into a particular subject was too great when looking at necessity and proportionality. That is the kind of discussion that we have now.

If you got to a position where, having gone through that process, the judicial commissioner still disagreed, the Secretary of State can ask the investigatory powers commissioner to look at this. If the investigatory powers commissioner disagrees, that is as far as that will go and the warrant will not come into force if they disagree.

Mr David Hanson: What of that discourse would at any time eventually be public in the event of accountability for one or both of those officials being held by the House of Commons or the House of Lords?

Paul Lincoln: If something went wrong, as we have seen in the past, inquiries are often held. The Intelligence and Security Committee led an inquiry into the circumstances surrounding the murder of Fusilier Lee Rigby, for example, which took into account the way in which these things work. Similarly, the commissioners hold to account an oversight of the process that is put in place.

Mr David Hanson: One final question. How many of these do you estimate would be deemed to be urgent, given what happened historically? What is your assessment of the number that will be urgent?

Paul Lincoln: In reality, we think that this will be very few percentage points of the overall number of cases. We have not provided a specific estimate, but it will be a very small number of cases—probably the majority would be where there is an imminent threat to life.

The Chairman: What about the definition of urgency? Is it self-defining or will we have some sort of guideline? I am sure that there will be grey areas.

Paul Lincoln: We have not set out in the Bill a definition of urgent. In reality, a warrant will be considered urgent only if there is a very limited window of opportunity to act. We would expect to set out guidance in a code of practice, as is usually the way in which these things are set out.

Lord Butler of Brockwell: If a warrant has been issued—

The Chairman: I do beg your pardon. We have to adjourn for five or 10 minutes while Members of the House of Lords vote.

The Committee suspended for a Division in the House of Lords.

The Chairman: We were in the middle of a sentence.

Lord Butler of Brockwell: If a warrant is issued for one purpose, can the information that it provides be used for another purpose? For example, if a warrant is taken out for someone suspected of terrorism and it throws up evidence of offences under Customs and Excise, could the information be used without taking out another warrant?

Paul Lincoln: Certain purposes are set out for the intelligence agencies where they are allowed to share information along the lines of their statutory purposes. If I take your example the other way around, if you discover in a tax evasion case that someone was involved in terrorism, the practice would be that you would take out a separate warrant to do with the terrorism and run the necessity and proportionality test for that.

Lord Butler of Brockwell: Thank you. But the information that was first obtained under the tax evasion warrant could then be used to justify a further warrant for terrorism but a further warrant would be needed.

Paul Lincoln: A further warrant would be the practice to be followed through. Yes.

Q7 **Dr Andrew Murrison**: I am worried about the five days, because the Five Eyes community does not put up an artificial distinction between urgent and routine, since all warrants have to be certified by a member of the judiciary rather than a politician. I wonder why we have lighted upon five days. Are we seriously saying that we may not be able to get a judge to pass a view within five days? I would find that extraordinary. Perhaps we might consider whether a lesser period of time was appropriate for matters that are deemed to be urgent.

Paul Lincoln: Among the various recommendations from the reports, the Royal United Services Institute report, for example, recommended a period of 14 days for an urgency procedure, which we considered too long. We alighted on a period of five days as a maximum that would allow for sufficient time when the system may be running at its hottest if there was a particular set of counterterrorism investigations going on. In reality, we would expect decisions to be made much more swiftly than that.

Lord Strasburger: We know that the Home Secretary signs on average six of these warrants a day. Could you tell us approximately how much time she spends on it?

Paul Lincoln: I cannot give you the precise time that she spends on each warrant. She has said to the House of Commons that she spends more time on warrantry than she does on any other topic.

The Chairman: Thank you very much. We now move on to Baroness Browning, who has a number of questions that she would like to ask.

Q8 Baroness Browning: Thank you. I have to remind the Committee of my interest in the register as chair of the Advisory Committee on Business Appointments, which gives advice to senior members of the security and intelligence community when they leave office. Could I ask you about the request filter system, which I think is new? Could you explain to us how the request filter system works for applications to access communications data? In explaining how that works, perhaps you might like to give us an idea as to the correlation between the new system and fishing expeditions and whether there is a vulnerability there.

Richard Alcock: The request filter is fundamentally a safeguard, the purpose of which is to limit the amount of data that goes through to law enforcement. People access comms data right now through a system of robust oversight, with the appropriate checks and balances and with necessity and proportionality at its heart. The request filter cannot be used unless a particular case has been made that it is both necessary and proportionate. By way of example of how the request filter might be used, a criminal may have committed three crimes in three locations at three different times. A request for comms data may go in about who was at a particular location in those three instances. Without the request filter and subject, obviously, to the approval being granted for that kind of request, the full array of data would be made available to law enforcement. The request filter would filter out all the irrelevant data and just identify the individuals or entities that were in those three locations at that particular point in time, so it would reduce the amount of irrelevant information that would go through to law enforcement. It does not allow for fishing, just to address that point, because you can only make a request when that is necessary and proportionate for a specific instance, which is obviously judged by investigating officers and with the appropriate oversight.

Baroness Browning: You do not think there is any fishing risk at all in the system.

Richard Alcock: No, because the same tests apply to the existing comms data approval regime.

Paul Lincoln: It may be worth adding that the Bill provides for a new offence around the abuse of powers around communications data; it provides a criminal offence for people who abuse the powers as part of this.

Baroness Browning: The Joint Committee on the Draft Communications Data Bill, as you are probably aware, identified a risk to the request filter system. Why do you think there is a difference of opinion? What has changed to minimise that risk?

Richard Alcock: The Joint Committee concluded that it was a safeguard while acknowledging that there was a risk. The risk has been mitigated by virtue of the criminal

sanction that may be imposed with inappropriate access to the information that could be accessed through the system.

Baroness Browning: Sorry, did you say "criminal sanction"?

Richard Alcock: The new offence, which Paul just outlined, of inappropriate access to comms data mitigates that risk.

Paul Lincoln: There is oversight by the Investigatory Powers Commissioner as a starting point in terms of all the powers in the Bill, but in addition to that we have greater defence in the Bill to make sure that in extremis if you are wilfully trying to abuse the system, a criminal sanction is available. There are also administrative and other sanctions available to the Government.

Q9 Lord Hart of Chilton: This is a question about judicial review principles. We know that the judge or judicial commissioner, when looking at the warrant, must apply the same principles as would be applied by a court on an application for judicial review. We have seen that there are some who say that that is not a great power because it is interested in process rather than the merits. I would like you to help the Committee by explaining what you understand to be the judicial review principles for the purposes of the Bill.

Paul Lincoln: As we said before, the Bill allows for a double-lock process. The judicial commissioner comes second in that process. The principle of judicial review is well established. Lord Pannick in particular set out that he thought that the test that was set for this Bill was the right one. In examining the data that is put in front of them as part of the request, they will see exactly the same information as the Secretary of State has and they will be able to determine whether or not the decision was lawful and rational. In doing so, they will also be able to determine whether or not the particular action was both necessary and proportionate. The necessary and proportionate test is, of course, exactly the same one that the Secretary of State is looking at.

Lord Hart of Chilton: We have seen David Pannick's article from 12 November, but we are interested in finding out the extent to which a judge could use what is called the Wednesbury principle in deciding whether or not no reasonable Secretary of State could come to the conclusion that a warrant was justified. Does the Wednesbury principle apply in this case, as that is a judicial review principle?

Paul Lincoln: The specifics here are that two things will be critical: first, that they decide in the first place that the action is rational and lawful; and, secondly, that it is necessary and proportionate. Those are exactly the same tests as the ones the Secretary of State will be looking at.

Lord Hart of Chilton: But how far could the judge go in deciding that the Secretary of State had stepped outside the remit?

Paul Lincoln: If a judge thinks that the Secretary of State has stepped outside the remit, it is for them to decide so and to say that they do not think that the warrant should come into force. Then there is the process that we described earlier about whether we appeal after that.

Lord Butler of Brockwell: What is the difference, if any, between "rational" and "reasonable"?

Paul Lincoln: I will have to ask one of my legal colleagues and write to the Committee on that one.

Lord Butler of Brockwell: It is an important point, because, as Lord Hart said, the question is whether the Wednesbury test—that no reasonable Minister could have taken the decision—should be applied. If I may say so, I do not think that you answered that. You used the word "rational", but what we really want to know is whether the Wednesbury principle applies.

Paul Lincoln: Okay. We will come back on the specifics of the principle.

Q10 **Dr Andrew Murrison**: On the subject of targeted interception warrants, if I had applied for and had been granted such a warrant but I wanted to change it in some way, how would I go about doing it?

Paul Lincoln: A process is set out as part of the draft Bill stating how modifications can be made to a targeted interception warrant.

Dr Andrew Murrison: Presumably those would be of a minor nature, or would they be fundamental?

Paul Lincoln: As for making a change to a warrant, if I was a criminal or a terrorist, let us say, and a decision had already been made by a Secretary of State and a judicial commissioner to put my communications under interception, then the decision had been made that it was both necessary and proportionate to intercept Paul Lincoln's communications in that manner. The example in that situation might be that I decide that I am going to buy a new mobile phone and, in doing so, I now have a new telephone number. Rather than necessarily going back and testing again that I am somebody who needs to have my communications intercepted, a senior official could make the change to say that that new telephone number could be added to that warrant.

Dr Andrew Murrison: At what point would you need to have the involvement of, first, the Secretary of State and, secondly, a judicial person?

Paul Lincoln: If you were to have situation where you then said—I do not know—a new person was coming along and a new circumstance, you would ask for a new interception warrant.

Dr Andrew Murrison: Through the whole process, so both the Minister and the judge?

Paul Lincoln: For both the Minister and the judge.

Dr Andrew Murrison: How does that differ from the situation that applies to equipment interference warrants?

Lewis Neal: It definitely needs some of the approach to modifications. Equipment interference follows the approach that we have taken to the original decision. In the case of SIA it will go through the departments of state, the Foreign Secretary and the judicial commissioner, whereas for law enforcement it will go straight to the judicial commissioner.

Dr Andrew Murrison: So why the difference?

Paul Lincoln: The approach follows the style point in how the authorising is done. In a case involving the intelligence agencies, for example, there is already someone separate from the chain of investigation who is looking at authorising that. In the case of the police, you are looking at doing this to add that additional safeguard as part of that process.

Dr Andrew Murrison: Presumably, there is also someone in the police looking at this too.

Paul Lincoln: Yes. Sorry.

Dr Andrew Murrison: You suggested that the difference was because in the intelligence agencies there is a specific person dealing with this.

Paul Lincoln: But you then have a separate department of state, which is independent from the body that is looking at it, which also considers that separately, whereas in the police you have that organisation itself looking at it rather than saying that there is a department of state, for example, separately looking at the authorisation. It is an additional safeguard.

Dr Andrew Murrison: Otherwise you just have the one.

Paul Lincoln: Otherwise you just have the one.

Dr Andrew Murrison: Do you think that is sufficient? It sounds a little odd to me.

Paul Lincoln: It effectively provides a form of a double-lock in terms of those modifications.

Dr Andrew Murrison: Why, then, should the handling of the equipment interference warrants and the targeted interception warrants be so different?

Paul Lincoln: That reflects effectively the starting point in saying who should be required to authorise that, and it follows consistently the starting point from—

Dr Andrew Murrison: It just seems to me that it unnecessarily complicates it.

Paul Lincoln: Our intention was to keep it simple.

Dr Andrew Murrison: Obviously it did not work. It has confused me. I admit that I am only a simple soul, but it seems to have established the two on different levels with different procedures. I wonder whether the matter might be simplified by simply having the same process without distinguishing it.

Paul Lincoln: That may be a judgment the Committee comes to.

Dr Andrew Murrison: Would it be a major issue in terms of workload?

Paul Lincoln: We would obviously look at what the implications might be in detail.

Q11 Lord Strasburger: Why does the phrase “judicial review” in respect of warrants appear in the draft Bill?

Paul Lincoln: We have talked about that by saying that those are the principles under which a judicial commissioner would look at the authorisation of—

Lord Strasburger: I am just trying to understand why the judge would not look on the same basis as the Home Secretary.

Paul Lincoln: As I said, the consideration they will give follows the point about whether it is rational and lawful, and whether it is necessary and proportionate, which is the same test as the one the Home Secretary or the Foreign Secretary applies.

Lord Strasburger: So most judicial reviews are rather redundant, are they not?

Paul Lincoln: I think we said that we would write back on the specific principle. As I said, we are quoting both the report from RUSI, which said that this was an appropriate way to approach this, and some of the recommendations made by David Anderson. In this space, this seems to be the appropriate approach to take.

Q12 **Suella Fernandes**: Before the judge reviews a decision, how will the evidence before that judge compare to the evidence before the Minister?

Paul Lincoln: The judicial commissioner will have the same information as the Secretary of State.

Suella Fernandes: How does the test applied by the judge compare to that applied by the Minister?

Paul Lincoln: They will look at the rationality and lawfulness, and will consider the necessity as part of that decision.

Stuart C McDonald: Will the judicial commissioner be able to question members of the intelligence services, for example, when considering warrants?

Paul Lincoln: You would expect there to be potential for some conversation to go on. At the moment, conversations would happen with the agencies to try to clarify potentially the methods that people are using. If someone was trying to conduct surveillance or an intrusive activity against a particular suspect, you may question whether collateral intrusion was appropriate. Those are the kinds of conversations that happen now. You would expect similar conversations in the future.

The Chairman: To clarify that, when authorising a warrant, clearly the judicial commissioner and the Secretary of State need not be together physically. They could be in different buildings and different places, but would it be at more or less at the same time?

Paul Lincoln: When looking at the warrant itself?

The Chairman: Yes.

Paul Lincoln: Not necessarily. For more routine warrants, it may be a period of days before a judicial commissioner can do it.

The Chairman: Would that be the five days that we talked about?

Paul Lincoln: It could be a number of days.

Lord Hart of Chilton: Unlike the judicial review normally, there would be no third party representations, would there?

Paul Lincoln: The investigatory powers commissioners could look at the system and decide whether they think this is something on which they need further representation. We have not put a system in a place where we are expecting people to be making additional submissions on top of those provided. We have said that we will provide training to those who will become judicial commissioners, and we are working with the Lord Chief Justice's office to set out what that might be.

The Chairman: Who would look at the warrant first?

Paul Lincoln: The process is that the final person who has the say is the judicial commissioner. It will have gone through a Secretary of State first.

The Chairman: The Secretary of State and then the judicial commissioner.

Q13 **Shabana Mahmood**: I just want to look at the issue in relation to privilege. Obviously, Clause 16 relates to Members of Parliament and the additional safeguards that will apply to communications between a constituent and an MP. I was interested in the rationale for giving those additional safeguards for Members of Parliament but not for legally privileged communications between a client and a lawyer or the protection of journalistic sources. What is the reason for the differential treatment of all three things, which are quite important to our constitutional arrangements?

Paul Lincoln: The Bill provides now for all forms of interception. The requirement of a judicial commissioner to sign off is the key difference from the situation today. All forms of interception now require the involvement of a judicial commissioner. That is a significant step that people would appreciate. The difference with Members of Parliament is that it also requires consultation with the Prime Minister, which reflects the wishes of certainly Members of the House of Commons. There was a debate about that some weeks ago on the Wilson doctrine, which went to the Investigatory Powers Tribunal. This is the result of those debates.

Q14 **Shabana Mahmood**: Moving on to communications data, which is about context rather than content, as a lay person I would expect content to be the most valuable bit of what you might be looking for, but the context has also been described as gold dust. It is very important. How would you describe the relative value of context as opposed to content when it comes to communications data?

Paul Lincoln: Both forms are very important but in their own different ways. For example, communications data is used in 95%[1] of all criminal prosecutions. It is an essential tool for law enforcement in particular to identify, for example, missing persons or to rule people

[1] Witness correction: the figure refers to 95% of serious and organised crime cases, handled by the Crown Prosecution Service

out of an investigation and try to minimise more intrusive techniques to gain content from that. It is very valuable in its own right.

Shabana Mahmood: So the oversight regime is less stringent than it would be for content. Given that you are both saying that they are both valuable, why is there different treatment when it comes to oversight?

Paul Lincoln: Oversight is by the Investigatory Powers Commissioner in all senses and all the powers in the Bill. There is perhaps a question about the authorisation, which you talked about, where Parliament has traditionally said that communications data is a less intrusive form than content, and the authorisation regime that maintains a very similar process that we have today reflects that.

Shabana Mahmood: Do you agree that it is a less intrusive form?

Paul Lincoln: Personally I do, and the Government have reflected that in the way in which the Bill has been put together.

Shabana Mahmood: Is that view shared across your sector, as it were?

Paul Lincoln: Yes. Law enforcement and the intelligence agencies will say that that is the same.

Q15 **Shabana Mahmood**: What is the rationale for Schedule 4? I can understand why police forces and intelligence agencies need to have access to communications data or are entitled to see acquisition of the data. I was slightly nonplussed by local authorities being on that list, given that by 2020 it would be a big deal if they can trim a tree or fill a pothole, rather than acquiring communications data, which might be beyond their resources.

Paul Lincoln: A wide range of bodies have access to communications data. The Financial Conduct Authority might use it for conducting investigations into insider trading. The Maritime and Coastguard Agency might use it for finding missing people at sea. For local authorities, ways in which to investigate might include rogue traders, environmental offences or benefit fraud.

David Anderson said that if you have relevant criminal investigation powers you should have the tools associated with that, and communications data is one of them.

Lord Hart of Chilton: Just one point. I did not quite get the answer to the question about the justification for allowing legally privileged communications to be intercepted. As you probably know, the Bar Council has raised strong objections to the fact that privileged communications between an individual and a lawyer are not safeguarded. Why is that?

Paul Lincoln: Special considerations apply to legally privileged material. Their safeguards are set out in codes of practice as part of this. Unfortunately, there may be situations in which people try to abuse the privileges available to them. Therefore, there is not a complete bar on such activity in terms of interception.[2]

[2] Home Office clarification: The policy intent is to make clear that special considerations apply to legally privileged material. The additional safeguards that apply to this and other particularly confidential information are set out in codes of practice. This is because the privilege attached to the contents of communications

Lord Hart of Chilton: Some might not consider that to be sufficiently justifying it, but that is the answer. Thank you.

Q16 Lord Butler of Brockwell: I understood that the Home Secretary said in her statement that local authorities would no longer have access to communications data, and I cannot find them in Schedule 4. Could local authorities in certain circumstances select this data?

Paul Lincoln: There are two points there. Local authorities have to go to a magistrate before they are able to access communications data. That was introduced in, I think, 2012. There have been some instances where potentially the powers have been abused. Part of the rectification of that was to bring in a magistrate.

The second question is probably to do with internet connection records, where the Home Secretary is on record as saying that local authorities will not be allowed access to internet connection records for any purpose.

Q17 Lord Strasburger: Are you aware that most experts consider communications data, especially that including internet connection records, to be at least as revealing as content these days? A former NSA general counsel said that it absolutely told you everything about someone's life and that if you have enough metadata you do not need content. A former director of the CIA said, "We kill people on the basis of metadata". Do not the most intrusive elements in communications data need a higher level of authorisation than the current entirely internal process?

Paul Lincoln: We agree that parts of communications data are more intrusive than others. As part of that, the Bill sets out the different authorisation levels, which are internal authorisation levels, with those that are more intrusive having to be signed off by a higher person in terms of the rank structure in any given organisation recognising the sensitivities behind it.

Q18 Dr Andrew Murrison: Can I just press you a bit on communications data and the long list of authorities that have access to this. I think you are referring in 2012 to the case that Poole Borough Council lost at tribunal, where it was found to have overstepped the mark.

Do you feel it is sufficient for these authorities to apply simply to a magistrate to gain the access that they say they require, or do you think that list needs to be revised? I certainly know which I think.

Paul Lincoln: Our approach has been to continue the process which requires a magistrate to sign off, which is an additional level to what it would be in other organisations. On top of that they have to go through a mandated single point of contact for quality assurance before going to make the request. The National Anti-Fraud Network is part of that, which has been pretty successful, and David Anderson recommends the NAFN as one of the most successful bodies in this area.

---

between lawyer and client is important and must be protected. However, it is in the nature of the intercepting agencies' work that they will sometimes legitimately need to intercept communications between people and their lawyers in the interests of preventing or investigating serious crime or terrorist activity.

Dr Andrew Murrison: Do you feel that their access to this data will mean that their skills in other means of detecting fraud might become degraded? Do you agree that fraud covers a whole load of things from the most serious crime to the frankly trivial?

Paul Lincoln: To put the numbers into perspective, only 0.5% of requests made for communications data overall are made by local authorities. It is a relatively low number in comparison with investigations in the round.

Dr Andrew Murrison: That is no justification though, is it?

Paul Lincoln: For access in their own right?

Dr Andrew Murrison: Not ensuring the job that we have to do to scrutinise this legislation at this stage would not be justification for us to overlook this particular thing; simply to say that it is so small that it does not really matter?

Paul Lincoln: I was not suggesting that. But in terms of the safeguards put behind this, certainly the Government have responded to that previously, and we have kept the same method, which involves the magistrate and the single point of contact through the National Anti-Fraud Network.

The Chairman: Can we move now to Miss Fernandes? Is your voice holding up?

Q19 **Suella Fernandes**: I think it is getting worse. Why has 12 months has been chosen as the timeframe for data retention?

Paul Lincoln: You could choose a range of different periods for which you might have retention. The data retention directive previously allowed for a timeframe between six months and 24 months. The UK decided to adopt a maximum of 12 months when it first introduced its legislation in this area. The 12 months was considered to be the right balance as to the level of intrusiveness in holding that amount of data. It was done on the basis of surveys by looking into the way in which law enforcement used the powers.

The critical reason for going up to 12 months is child sexual exploitation cases. Certainly when a survey was done on this in 2012, 49% of all requests made in child sexual exploitation cases were for data between 10 and 12 months old. That is a very significant period, which is reflected in the position that we have taken.

Suella Fernandes: What assessment has the Home Office made of 18 months?

Paul Lincoln: You could go further than that, but this is the position that we have taken historically. Other nations have gone further. The Australians are a good example. They recently passed legislation to go for 24 months' worth of data retention, but we thought that 12 months struck the right kind of balance between those two things.

Suella Fernandes: In terms of communications service providers and their holding of data for 12 months, has there been any assessment of the cost and workability of that?

Richard Alcock: As you would expect, we have had a number of meetings with the communications service providers on which we would likely serve notice under the new

legislation. The retention period in the Bill obviously reflects the retention period proposed in this legislation. We have a very good relationship with the CSPs on which we serve notices now. We have worked with them throughout the summer, and before then, to think about the likely data volumes and to work out the estimated costs for the retention of internet connection records specifically. Those are contained within the impact assessment.

It is important to note that it is an estimate. Why is it an estimate? That is because CSPs systems change all the time. There are mergers, acquisitions and so on, but it is the best estimate right now based on the work that we have been doing with them over the past few months.

Paul Lincoln: It is also worth clarifying that the period for a maximum of 12 months for communications data is already current practice in terms of data being stored by those that are under a data retention notice. So that is not a new proposal.

The Chairman: You said earlier that one of the reasons for the 12 months was the investigation into child abuse, but you also implied by that that other investigations might not need the retention for 12 months. Could there be a sliding scale of holding this material according to the nature of the investigation?

Paul Lincoln: There is a question, therefore, between retention and access. To be in a position where you can access data in relation to child sexual exploitation, you have to retain all data associated with communications for up to 12 months to able to make those connections. The question of access is then perhaps complicated in terms of practicality. You may end up missing a significant proportion of investigations. If I was to say that a firearms investigation needed data that was six months old, I might make a connection to a child sexual exploitation case that also needed nine to 10-months-old data, or to a prostitution ring that needed something else, and I would not necessarily be able to make the links between those different investigations by having access for different times.

Mr David Hanson: Can I just be clear? You said that the costs in the impact assessment are to cover the costs of the 12-month period. Are the Government entirely covering costs to service providers and any expanded retentions?

Richard Alcock: The costs are to cover reasonable costs for the additional retention of the internet connection records, so there is provision in the—

Mr David Hanson: So how much is the impact assessment figure? From memory, around £240 million is related to that cost.

Richard Alcock: It is £174 million over a 10-year period in relation to internet connection records. Right now, under existing legislation, in the last financial year we spent around £19 million on data retention, so broadly speaking we are doubling the cost of data retention.

Mr David Hanson: So, again, does the assessment over the 10-year period include an assessment of the expansion of the market, of different types of material, of different types of activity, of the capacity overall of organisations, of new providers entering the market? How do you arrive at that figure?

Richard Alcock: We have worked with industry over summer to look at the likely data volumes and the costs associated with that volumetric growth over time, so even though I gave the example of £17 million a year, the reality is that the cost may go up over that time. But, as I say, we have been working very closely with the comms service providers on which we are likely to serve notice to underpin the facts and figures within the impact assessment.

Mr David Hanson: So when we have the service providers in front of us in the near future and we ask them the same question, will they tell us that they are content with the amount of resource that they give them, or not?

Richard Alcock: As I say, we continue to work with the comms service providers to look at the estimates of volumetric growth and how we would go about implementing those systems over time. We make balanced judgments on the service providers on which we serve notices, and we sometimes have to make hard choices about where we put data retention notices. But, again, as I say, it is all about working very closely with law enforcement, to identify where most value can be accrued from retention, and with comms service providers to understand—

Mr David Hanson: One final question from me. Is that therefore a budget that you have to spend, or is that an assessment of the costs?

Richard Alcock: It is currently an estimate of the likely cost for implementing internet connection records over a 10-year period.

Mr David Hanson: With certain providers.

Richard Alcock: Yes.

Lord Butler of Brockwell: Why does the taxpayer have to meet the cost at all of these records being retained? Why can it not simply be a condition of providers providing services that they retain these records at their expense?

Paul Lincoln: What we have tried to do, and as we have done in the past, is to make sure that companies are not materially disadvantaged by having to meet the requirements of government in this space.

Stuart C McDonald: Just a quick follow-up question first of all. I was interested in what you said about doing surveys of police work in relation to retained data. You commented on the 49% of all requests in child sexual exploitation cases being for data between 10 and 12 months old. In how many cases where the data was between 10 and 12 months old did that data prove to be essential to the outcome of the case?

Paul Lincoln: You are probably better asking the law-enforcement colleagues who are giving evidence after us, but communications data is often the only start point for child sexual exploitation investigations.

Stuart C McDonald: Thank you very much. Also in relation to data retention, obviously one of people's key concerns is security. When you are retaining data on such a huge scale, how can you be sure that that data is going to be securely retained?

Richard Alcock: Our retention systems are built to meet stringent security requirements, working in partnership with comms service providers to ensure that they meet very rigorous standards. Those systems are overseen by the Information Commissioner. We have annual accreditation. We have, typically, dedicated stores in which the comms data is held, which can be accessed only by law enforcement through encrypted data links and so on. As I say, it is a high priority for us to ensure that security and integrity. We have a very good track record of maintaining the security of existing data retention systems, and we are looking very much to build on that good practice, working in partnership with the comms service providers.

Stuart C McDonald: A related concern is about the definition of service provider. Someone suggested that the way that is defined just now means that pretty much any form of software provider could end up being saddled with these obligations to retain records over 12 months old. Do you have a response to that concern?

Richard Alcock: We will not be putting notices on every service provider as you suggest; we make balanced judgments about which organisations we would serve retention notices. Obviously I cannot go into detail about the organisations that we would intend to serve notices on, but we have been working with every organisation that would be likely to have a notice served on it.

Paul Lincoln: It is also worth saying that there is a route of appeal for those organisations if they think that this is a disproportionate thing to do. They can appeal to the Secretary of State, and there is a process involving a technical advisory board, which will consider the technical implications and cross-implications as part of that.

Q20 **Stuart C McDonald**: My final related question is about whether or not it is going to place UK-based communications service providers at a competitive disadvantage, in that some non-UK citizens will simply choose not to trade with UK-based providers.

Paul Lincoln: Part of that question is similar to Lord Butler's question. In that respect, that is one of the reasons why we give reasonable costs back to the companies as part of that. Was there something else behind your question?

Stuart C McDonald: Not just in a financial sense but in the sense of the different obligations that are going to be placed on UK-based providers and non-UK-based providers. Some might simply say, "If there is going to be all this storage of my data, I'm just not going to use a UK-based provider".

Paul Lincoln: The powers in this are not new; they have been known about for some time. Data retention is a widespread power that is used in many different countries, so I would think that that set of differentiators is likely to be limited.

Q21 **Lord Butler of Brockwell**: Going on to one or two technical issues, we understand that because IP addresses are not unique, you cannot identify a sender solely through the IP

address, but you can identify them through the internet communications records: in other words, through what they have been to. So is it correct that providers keep records of internet connections?

Richard Alcock: Some do not at the moment. The purpose of the legislation is to ensure that they can where served under notice. The whole operation of communications over the internet is very complex. If you will indulge me, if you have a smartphone, that phone will then communicate with your comms service provider and you will have an IP address and what is known as a port address between those two nodes. There will then be another IP address and another port address between your comms service provider and the destination, whatever web service it is. So you have constantly changing IP addresses and port numbers, and because of that sometimes having the destination IP address or the internet connection record address is the only way of identifying a person to a communication.

Lord Butler of Brockwell: So have you reached agreement with the providers on how this is going to work technically? Do you have a clear agreement with them about what you are going to serve notices on for retention?

Richard Alcock: We have ongoing discussions with a number of comms service providers, as I mentioned before. Those service-provider systems are constantly changing. We have a good relationship with the service providers on which we are likely to serve notice, and we have a good understanding of their current technical systems. During all the conversations that we have with them, at no point have they said that it is impossible to implement.

Lord Butler of Brockwell: So when we see them, will we hear from them that they think that the exercise of these powers is practicable?

Richard Alcock: I hope they will say it is possible. They will say it is hard. They will say that there is more work to be done, because their systems are constantly changing. But, as I say, we have been having a productive dialogue with them for a number of months, specifically about internet connection records.

Q22 Lord Strasburger: Before I ask my question, I should mention that the Home Office estimate for the cost of implementing the communications data programme, which in terms of storage was considerably smaller, was, from recollection, £1.8 billion over 10 years.

I want to talk about security. There are many breaches of cybersecurity every week. Examples from the last few months include: TalkTalk; giffgaff; a 13 year-old boy hacking into the email account of the current director of the CIA and accessing sensitive government data; and the theft of 4 million personnel records of US government employees, probably by the Chinese. How can the public have any confidence that their personal data, stored by the Government at their ISPs, will not be stolen, and who will be responsible when it is?

Richard Alcock: The retention systems are built to stringent standards, and those standards are set by the Home Office. Systems do not go live unless they have been independently tested and accredited. We are very confident in the arrangements that we have to maintain security of the data retention systems, and I cannot say more than that. We completely

understand the threat, and because of that we put a lot of effort into ensuring that integrity.

Lord Strasburger: Who advises on that?

Paul Lincoln: We do not want to sound complacent, but the Information Commission provides independent oversight of those arrangements. As I say, it is one of four principal things that we look at: the physical security of buildings, infrastructure and the rest of it; technical systems, including firewalls and the like; personnel vetting systems, where that might be appropriate; and procedure—the processes, training and the like, which are put behind that.

Richard Alcock: And all that is accredited on an annual basis.

Q23 **Matt Warman:** I would like to talk a bit about encryption. We all know that, on the one hand, encryption is absolutely essential for everyday life. On the other hand it has also meant that some bits of communication that you were able to access are now not visible. There is provision in the Bill for the Secretary of State to make regulations to impose obligations on telecommunications service providers "relating to the removal of electronic protection applied by a relevant operator to any communications or data". Does that mean that there is provision here to remove encryption, and, if so, how?

Paul Lincoln: I should start by saying that the Government are a strong supporter of encryption for information audit purposes and information assurance purposes. Some £860 million was spent on the national cybersecurity programme, and of course the spending review last week announced another £1.9 billion for looking at this. GCHQ probably does more for this country's cybersecurity than any organisation.

The Bill itself in effect replicates the existing legislation, which has been in place since 2000, and says in effect that we should be in a similar position to that of the real, physical world, where, as David Anderson says in his report and others have said, you do not want there to be places where people are allowed to go unpoliced and ungoverned. The same should apply in the internet world. So when you have taken the steps with regard to necessity and proportionality, you can place a requirement on companies to provide you with content in the clear.

Matt Warman: I understand that you might wish that to be the case, but in practice everything from my message from an iPhone to another iPhone is now encrypted end to end. Does this provision propose to tackle something like that, and, if so, how?

Paul Lincoln: Not everything is encrypted end to end. It would not suit the business models of many companies to encrypt their information end to end, and many of those companies would not tell you that their systems were unsafe, which they are not. But you have to think whether or not in the right circumstances you will ask people to unencrypt information, and people do do that for us.

Matt Warman: Where companies currently think it is right to provide a commercial service that involves end-to-end encryption, are you trying to tackle that, and, if so, how?

Paul Lincoln: All we have done is replicate exactly the same service. If you are providing a service to UK customers and the Secretary of State and a judicial commissioner think there is necessity and proportionality in order to be able to provide that information, those companies should be required to provide that information in the clear.

Matt Warman: Do you think that is practicable?

Paul Lincoln: We are not setting out for anyone how they should do that. It is for others to say what the best way is for them to achieve that. The Government do not want to hold the keys to encryption or anything like that. That debate happened a long time ago. The Government decided that they did not want to do that and have not set out technical standards in this regard. They are saying, "In the right circumstances, we want you to be able to provide this information in the clear".

Q24 **Matt Warman:** I will come on to bulk equipment interference in that case. Could you all outline what bulk equipment interference is as far as you are concerned, and when it might be proportionate?

Lewis Neal: There is a difference between targeted equipment interference and bulk equipment interference. For targeted equipment interference, you might know the identity of the individual or the piece of equipment you are targeting. For bulk equipment interference, which is targeted at activity overseas and where the intelligence picture and the levels of information about your target are less, you would be able to seek authorisation to target equipment where you did not necessarily know a particular device or the individual that you were targeting.

Matt Warman: And when might that be a proportionate response?

Lewis Neal: Where you have a specific intelligence requirement overseas and you do not have the information but you might have an idea of the locality of the risk or the threat, the necessity would be set out and you would consider the proportionality of that action and potentially the types of information that you were seeking to obtain. Typically in that situation you might look at equipment data that enabled you to further identify the target and to develop a case for activities that have a higher level of intrusion.

Matt Warman: So you would see equipment interference in lay terms as happening at the level of internet infrastructure, rather than—

The Chairman: Order, order. There is a Division in the House of Lords. We will be back in 10 minutes.

The Committee suspended for a Division in the House of Lords.

The Chairman: Again, apologies for democracy. Perhaps I may move now to Miss Atkins who I know has a number of questions.

Q25 **Victoria Atkins:** How does the data collected as a result of equipment interference differ from interception material?

Lewis Neal: Equipment interference is a range of techniques to acquire communication information from a variety of bits of equipment, from computers to mobile phones, whereas interception is making communications available while they are in transit. In practice you could use both tools to obtain the same levels of information, be it equipment data, communications data or content, but that would depend on your objective and exactly how you were using the tools.

The legislation will require the agencies and the Secretary of State to consider the most proportionate way to acquire the data. If equipment interference may enable you to collect a certain bit of data, essentially you would use that technique as opposed to using interception where you may be collecting more data and a higher level of intrusion when it is not proportionate.

Victoria Atkins: Intercept material is not admissible, or indeed disclosable, in court legal proceedings. Why is it deemed acceptable for material acquired through equipment interference to be eligible for use in legal proceedings but not material acquired through interception?

Paul Lincoln: In principle the Government have no objection to having interception used in evidence. It is the default that you would want to have material used in evidence, but there have been a number of reviews into this over the years. The last was in December 2014, which concluded that it was not possible to introduce an intercept-as-evidence regime in this country. The benefits would not outweigh the risks and the costs associated with doing so. There have been seven or eight reports on this, which have all come to that same conclusion.

Victoria Atkins: I know that colleagues might be wondering why intercept materials is admissible in other countries under different regimes. Is it fair to say that those countries have different disclosure regimes that perhaps are not as demanding of law enforcement and prosecution agencies as the disclosure regime in this country?

Paul Lincoln: There is a combination of questions about disclosure. In particular, if you were to intercept someone's communications and were trying to use that in court, you would potentially need to intercept every bit of communication that they have done and transcribe all that so that you could set out whether or not there was information that was contrary to that that would be used to bring a prosecution. There are other ways in which other countries' regimes differ. We are not the only country in the world: for example, the Irish do not have an intercept-as-evidence regime either.

The Chairman: Thank you very much indeed. I am sorry that it has been a bit disjointed, but it has been an extremely valuable and interesting session. Many thanks for your time.

Lord Strasburger: Chair, may I correct my statement? I should have declared an interest. I have been a member of Liberty since I was a young man.

The Chairman: Thank you very much indeed.

Erka Koivunen, Cyber Security Adviser, F-Secure Corporation (QQ 207-215)

Evidence heard in public Questions 207-215

Oral Evidence

Taken before the Joint Committee

on Monday 21 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Suella Fernandes MP, David Hanson MP, Shabana Mahmood MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Lord Hart of Chilton, and Lord Strasburger.

Witness: **Erka Koivunen**, Cyber Security Adviser, F-Secure Corporation, gave evidence.

Q207 **The Chairman**: A very warm welcome to all three of you. Particularly as we are so close to Christmas, it is very good of you to come along and give us the benefits of what I know is your considerable expertise, knowledge and experience. We very much look forward to listening to you. I will start by asking you a general question, which will give you the opportunity, if you so wish, to make any general statements about the Bill. Will it work? What are your views on the draft Bill from a technical standpoint and are these proposed powers workable? Perhaps we will start with Professor Buchanan.

Professor Bill Buchanan: Thank you. I would say that we live in a very different world from the one that we did. We have built this cyberage within about 40 years, but the infrastructure that we have created is very fragile. We must protect citizens from hackers and so on. We must protect privacy and identity. More and more services are moving towards the provision of both privacy and identity. Individuals need to be assured that they are not being spied on by cybercriminals across the world. They also need to be able to prove their own identity and the identity of what they are connecting to.

Encryption involves both these aspects. It keeps things private but it increasingly is also used for identity provision. Much of cryptography is now focused on proving the identity of the services that we connect to. Just now, most of the services that we use in the cloud—Google, Amazon, Facebook and so on—are encrypted. Every time we see "https" and we see a green bar on our browser, it means that we are protected with a unique cryptography key for every session that we create. It is almost impossible to crack that key without knowing the private key of the site to which we are connected. The only way that someone could crack communications through a tunnel such as that is to get the private key off the company that is involved in the communications, which would involve Microsoft, Facebook, Twitter and so on handing over their private keys. The problem around that is that if someone gets access to those private keys—those special keys—we open up the whole of the internet and we will have the largest data breach that has ever been caused.

The communications that we have are obviously highly sensitive. The logs that we see on the internet are really the history of our whole lives. They are our thoughts, beliefs and dreams almost by the second. Every single thing that we do is recorded in our web history.

The amount of money that that would be worth to a criminal—a cyberhacker on the internet—would be almost unlimited. If an ISP was hacked, you can imagine what the logs could be used for and what bribery there could be for individuals and companies. A balance needs to be struck between the privacy of individuals, the protection of our businesses and the risk of serious organised crime.

Erka Koivunen: Lord Chairman, it is an honour to be present in this Committee session. It has been a fascinating journey to read through the Bill, in particular as a non-native speaker—it has been a tedious task. However, I would like to offer my congratulations. The Bill is pretty transparent in the way in which it lays out the intentions of the Government to do a lot in terms of law enforcement and signals intelligence. This is a Bill that you would get if you asked signals intelligence organisations what they would like as a Christmas present; they would reply that they wanted this and wanted it in bulk.

However, there are some unintended consequences when writing broad legislation that would give such exceptional powers to intelligence agencies and law enforcement. If there ever was a question whether nation states, Governments and military organisations would be engaging in hacking and computer intrusions, I guess that this Bill solidly sates that, yes, this is what they do and this is what the UK Government are actively seeking to do. Frankly, this is something that has been going on for quite a while now. The Bill is an attempt to put the existing situation in writing. We, as a provider of cybersecurity services to private companies and Governments, would typically advise our customers to be aware of criminal activity taking place and of their organisations being targeted by nation states and Governments as well. No better marketing material for services such as those that we provide could be envisaged. We should be aware that the powers laid out in the Bill could be misused. This will lead other nation states to try to mimic these powers. As a member of the European Union—I come from Finland, I am a Finnish national and our company comes from Finland—I feel that I am now a target of many of the activities laid out in the Bill. I do not think that this is what I signed up to when I joined up the cybersecurity profession. There are lots of discussions on how to limit those powers. I am not a lawyer or a legal person, but there are lots of things I can imagine technically that would undermine our society's security. Some of the things that we build in our online systems depend on strong cryptography, in terms of encryption, authentication and authenticity.

The Chairman: Thank you so much indeed. It is very good in English and in Finnish. Mr King?

Eric King: I will not repeat any of the feelings and concerns that both Bill and Erka have highlighted, but perhaps I can help the Committee in one regard by focusing your minds not on the question of whether the proposed powers are necessarily workable, because the majority of them are in fact already in use. That is not to say that they are powers granted by Parliament—indeed, I would expressly say that that is not the case—but they are powers that our agencies have been deploying for a number of years.

It has only been this year for the most part that the public have found out about these and that they have been officially avowed. It was in February this year that the Government avowed hacking for the first time—it is now called "equipment interference". In the Investigatory Powers Tribunal a few weeks ago, I heard from government lawyers that bulk equipment interference apparently had still not been avowed. Bulk interception was only avowed with the writing of the ISC's report in March this year, for which we are very

grateful. The use of bulk personal data sets, as mentioned in the Bill, were again revealed to the public only with the ISC's report in March. The ISC stated at the time: "Until the publication of this Report, the capability was not publicly acknowledged, and there had been no public or Parliamentary consideration". Bulk communications data acquisition was only avowed on the very day that this Bill was introduced to Parliament by the Home Secretary, who admitted that our Security Service, MI5, had been acquiring in bulk the phone records of everyone in the United Kingdom. Anderson commented at the time to the BBC that the legal power that had been relied on to exercise that authority was so broad and the information surrounding it so slight that nobody knew that it was happening.

I make these points to say that the Government, in my mind, should make operational cases from first principles for every single one of these powers. Simply because they have already been in use and simply because the agencies have interpreted law in a manner that they feel has made them lawful does not make them lawful. It is right that Parliament should receive a full operational case for each and every one of these powers. It is a matter of assessing not whether they are merely helpful or offer some form of value, but whether, given the scope of everyone's lives that they touch—after all, that is what bulk powers do—they can be vetted and scrutinised to make sure that they are both necessary and proportionate.

The Chairman: Thank you all three very much indeed.

Q208 **Shabana Mahmood:** I want to ask you about future-proofing the Bill. When the police, Home Office and others gave evidence to us, they were pretty robust in their view that these powers were sufficiently future-proofed against behavioural and technological change, as the powers were broad and wide-ranging. Other experts, in evidence, scoffed at the very idea of future-proofing, because of the pace of change in technology and how that impacts on behaviour in the online and digital space. What are your views on whether future-proofing is possible and, if so, whether that has been achieved in the draft Bill?

Professor Bill Buchanan: If there is one change that is happening in systems just now, it is a move towards the cloud. So like it or not, most of our emails are stored in the cloud, possibly in other jurisdictions. The main moves are with tunnelled web access. If someone uses a tunnelled connection, you cannot see the detail of the information that is passed. The minute someone uses https there is no way that you can see what page they accessed on the site; you can see the IP address but you cannot see what they clicked on. The whole world is moving towards https. Google is almost forcing companies to sign with a digital certificate or they will not be ranked highly. Many companies are moving towards adding a digital certificate. There is now a service online for free; you do not have to pay for a certificate any more. So increasingly companies will be signing their sites. Once they do that, communications are likely to be https.

There may come a time when many service providers will accept only secure communication. It is likely that our old protocols—http, Telnet, SMTP—will be switched off and replaced by the s version, the secure version. More and more people are using VPN connections. If you are a businessperson you will use a VPN connection if you are on the road. VPNs cannot really be cracked at all. Along with that, more people are using proxy systems where the accesses are not coming from their own computer but from another computer. Increasingly we are using public wi-fi to access the internet. It is extremely

difficult to trace someone who connects to, say, Starbucks wi-fi. Very basic registration happens, usually around email addresses, and many users would not feel that they need to put full details behind that. The increasing usage of Tor is a particular problem. With Tor, you usually will not see anything at all about the IP address of the destination because each link on the chain is encrypted with a special key so there is no way you can see anything from a Tor connection.

Shabana Mahmood: So tunnelled access—such as VPNs, which many MPs use to log in when they are not on the Estate, for example, and public wi-fi—is becoming the default and therefore not easy to crack.

Professor Bill Buchanan: We have created an internet that is based on legacy protocols. They were created a time when someone had to type in the commands manually. We now have browsers, graphical interfaces and so on. These protocols can be easily breached. They can be sniffed. Anyone who listens to the traffic can crack them. So increasingly businesses and individuals are protecting themselves through the usage of tunnels. Certainly if you are a business you must ensure that your communications are encrypted over public access. If you stay in a hotel room, if you are using the public wi-fi, how do you actually know that the SSID you connect to really is the wi-fi of the hotel? It could be some intruder next door. It happened in the Far East: a whole lot of hackers in a hotel room targeted businesspeople and were continually sending vulnerabilities to them. More and more we are encrypting traffic and setting up tunnels, and it is very difficult for the UK to drive these things because they are typically driven by the cloud providers such as Microsoft, Apple and Facebook.

Shabana Mahmood: On the cloud, people with smartphones go up to the Apple cloud automatically and you get a certain amount of space. Is there any difference in security between the free cloud services and the paid-for ones such as Dropbox, as well as in how much space you get?

Professor Bill Buchanan: Obviously you pay for the security that you get. Brand reputation is very important in this space. Apple, Facebook, Microsoft and Google have their brands to protect. If there was a large-scale data breach for any of those companies, it would decimate them. Banks and the finance industry have invested a great deal in the UK in protecting data and have gone through the CBEST penetration testing. Other companies, such as retail companies and internet service providers, have not gone through the same type of testing.

Erka Koivunen: The question was about future-proofing the legislation. I was puzzled by the introduction of the term "communications service providers"—CSPs. I was not familiar with that. Internet service providers—ISPs—and the telecommunications operators; that is the normal, old-fashioned way of referring to those carrier and access network providers. I was equally puzzled to find that in the actual text of the legislation, CSPs are not mentioned. There are references to what telecommunications operators would need to do and what information would be requested from them. To me, this sounds a pretty old-fashioned way of approaching the problem of acquiring information about content or about whether an event took place in the first place. In that sense, I do not consider the Bill to be future-proof. Because there are so many references to bulk information gathering, it

seems as though there is not even a proper attempt to go to non-traditional telecommunications providers to acquire the material that would be needed. Instead, the information and the traffic would be collected from the wire in bulk and then content or metadata collected with brute force, if you will. Of course, the equipment interference provisions in the Bill acknowledge that whenever you are unable to decrypt the material that you get online from the wire, you will need to go to the end point of the communication, where the material will be stored—hopefully in clear text.

I should point out that our company is actually one of the providers of those VPN type of tunnelling services. We provide a service where you can analyse yourself and encrypt your communication. You are able to move yourself virtually around the world so as to hide the origin of your traffic. Currently, we get only a handful of "targeted" law enforcement requests for the activities of our end users. I guess I am at liberty to tell you that none of them this year came from the UK. In this sense, I am a bit puzzled as to why there is such a pronounced need to get bulk information when even the old-fashioned, more targeted means to acquire information from communications providers are not being used.

Eric King: As upsetting as I am sure it will be if every few years we have to go through a Bill of this length and size, it may be what is required. This is an area that is inherently unsuitable for future-proofing because every year technology simply provides us with possibilities that our laws do not cover squarely or clearly. Where there is a grey area, our agencies have interpreted the law to give themselves the most expansive authority time and time again. Michael Hayden, the former director of the National Security Agency in the US, summarised this by saying, "Give me the box you will allow me to operate in. I'm going to play to the very edges of that box". I am not sure I can criticise him for that. I think that the permission our agencies have is very important and it is right that they use every authority and every capability at their disposal. Nevertheless, it is important that they exercise those powers only when they have been clearly authorised to do so by Parliament.

There have been a number of circumstances over the past few years where in this country we have found that that has not been straightforwardly followed. To my surprise, in the course of litigation involving GCHQ, Charles Farr provided a statement to the court which provided an entirely novel interpretation of what constitutes an external communication. He told the court that if you and I were sending a message using our phones, that would be classed as internal, but as soon as we switched to Facebook, or any other online platform, you and I were no longer communicating. Instead, I was communicating with Facebook, and so were you, and as a result they were external communications. As a result of that, fewer protections were offered to both you and me. It seems to me that that is not right.

We had a similar experience with intelligence sharing. I will not repeat what I know you heard from Amnesty earlier on that point. More recently, I was concerned to learn that, in particular, GCHQ and our security services have taken a very expansive approach on their authorisation of what constitutes a targeted warrant. It seems that thematic warrantry has now become slightly more default than any of us were aware. I was in court a few weeks ago and heard the Treasury devil argue that the use of a general warrant—that is, that you could target on the basis of a class of persons—would be entirely permissible under the Government's current interpretation of the Intelligence Services Act, which they claim

provides them with the ability to hack domestically inside the United Kingdom. These are all issues that the intelligence agencies have thought about. They have determined in secret the scope of their authority, and they are being challenged in these circumstances only because of a whistleblower who brought them to public attention. They have been brought before the courts and they are being tested. It seems to me that we will need regularly to update this law if we do not want to encourage whistleblowers to continue their practices year on year.

Q209 Lord Strasburger: Professor Buchanan, you mentioned the risk if you are in hotel of not knowing whether you are communicating with the hotel's wi-fi or something else. I have been in that position and have had my phone intercepted. It was a demonstration that was organised by F-Secure, so I declare that interest.

On the subject of future-proofing, we have heard many times during these proceedings about the very broad way that various parts of this Bill and other Bills in the past have been drafted. The explanation that we hear from the Home Office is that this is to allow future-proofing so that it can massage the definitions as time goes by. Mr King mentioned this, but neither of the others did. Is the answer to have a new Bill every Parliament, which would be every five years?

Professor Bill Buchanan: I go back to my main point that I can see cryptography and the use of tunnels increasing. There is no Bill in the world that can crack an encryption key that has been created for every connection that you make. You can legislate for it, but technically, it is not possible. The state of the art is 72 bytes. If you tunnelled on every single computer in the whole world, in a month or so, you could just crack a 72-byte key. The keys we are now using are 128 bytes or 256 bytes. It is double, double, double, double until we get to 128. It would take you a lifetime to crack 128-byte keys with current technology.

The Chairman: Is that a yes or a no, Professor Buchanan? Do you think they should be?

Professor Bill Buchanan: I can only say from a technical point of view, from a cryptography point of view, that the Bill would have to provide that cloud service providers would have to hand over the private key, have a key in escrow or have some backdoor, some proxy, on a machine. That is the only way that you would crack the cryptography problem.

Lord Strasburger: I was not talking specifically about cryptography; I was talking about all the provisions in the Bill in order to keep the provisions of the Bill current. Do we need to come back to it roughly once every five years and have a new Bill?

Professor Bill Buchanan: Certainly the way that computing is moving the pace is unstoppable.

The Chairman: Mr King, Mr Koivunen, can you say briefly, as we are beginning to run out of time, whether you agree with Lord Strasburger that we as a legislature should be renewing these provisions every so often because of the changes in technology?

Erka Koivunen: Definitely. I am a big proponent of transparency and the democratic process. Intrusive methods, such as these, should be reviewed.

Eric King: Yes, although I do not think that that should lessen the scrutiny that is put in place for this Bill.

The Chairman: On the principle of renewal, all three of you—or two of you at least are not quite sure—would be in favour.

Q210 **Dr Andrew Murrison:** Do these keys exist, or would they have to be created?

Professor Bill Buchanan: Do you mean the keys of the tunnels that are created or the keys that are held by the cloud providers?

Dr Andrew Murrison: The keys that are held by cloud providers.

Professor Bill Buchanan: A survey was done recently of some of the largest companies in the world. They had an average of more than 17,000 encryption keys—key pairs, as we would call them. A public key is known by everyone, the private key is what you keep secret. If someone finds the private key, they can crack the communications. The majority of companies do not know how many keys they have. Keys are being created at any given time, but companies such as Google will have a master private key which is used for its communications. That key is updated regularly. It might be six months or one year or so. That key will stay active for that amount of time. There is a revocation service on the internet that does not quite work. If the keys have been stolen by someone, what is meant to happen is that all the browsers will no longer accept that key. Unfortunately, Google Chrome does not accept revocation services by default. The keys are actually created by the cloud providers, but every session we create with our cloud services has a new key every time.

Dr Andrew Murrison: I suppose that is our safety net, is it not? We are worried about government having this information, or having access to information through keys. However, the gist of what I am asking is, are we at the moment at the mercy of providers such as Google?

Professor Bill Buchanan: Yes.

Dr Andrew Murrison: Yes, thank you. That is no comfort, is it? There are a number of these, and we presumably have no control over their internal security mechanisms, except as far as their reputation is concerned.

Professor Bill Buchanan: Only 5 per cent of SMEs have any auditing facility with their cloud provider. Only about half of large companies have some form of auditing that they can actually have on cloud services.

Dr Andrew Murrison: Thank you. Can I ask you about definitions in the draft legislation that we have seen? We have a range of descriptions, particularly in relation to communications data, such as entity and events. You might be forgiven for thinking that Sir Humphrey had drafted some of these, because to a lay person they are certainly approaching meaningless. I would be interested in your thoughts on the definitions and whether you think that they are simply creating the aforementioned box and are drafted in such elastic terms as to be maximally obliging to those in the agencies who want to pursue this data. We have mentioned, for example, the thematic warrant. It is not entirely clear to me what a thematic warrant is,

and several witnesses have already said that they are concerned about the fluidity of some of the definitions used in the Bill. I would be interested in your views.

Eric King: As a broad, concerning criticism, the definitions here leave a lot of room for manoeuvre. On issues such as thematic warrantry, it is less the term "thematic warrantry" itself but the scope of the language surrounding that that worries me. The ability in particular to add and remove individuals seems very broad. The more technical terms "events" and "entities", while new to all of us, are not new to the Home Office; they are the terms that GCHQ itself has used for the past decade. GCHQ is very familiar with them and has been exploiting them to the full for a very long time. Events and entities in particular are the issues that are of most interest to our security agencies; these are the capabilities that provide them with the most amount of information. The ISC helpfully said earlier this year that, "the primary value to GCHQ … was not in the actual content of communications, but in the information associated with those communications". I can give you a longer list, but it is very important that these definitions are tightened. A number fall in the gap. As an example, if a telephone call is intercepted and GCHQ identifies the gender of the speaker, is that an event, an entity, content? It is unclear to me.

Q211 Suella Fernandes: Clause 12, Part 2, relates to interception and refers to related communications data. I should say that new Clause 12 replaces the existing Part 1, Chapter 1 of RIPA, so it is a power that already exists. With reference to the point about related communications data, in brief it relates to communications that have been intercepted in relation to the postal service and telecommunications systems, and to assisting with the identification of a telecommunications system, an event or a location. What is your view on the clarity in that clause of the term "related communications data"?

Professor Bill Buchanan: A key aspect of this is that the IP address can never really be trusted, and any digital information that you gain typically from a home environment or electronically, again, cannot be trusted. If someone is in a home environment, they are typically on a private network and they are mapped to a single IP address, so it is very difficult to pick off the person who is actually communicating. So the ability to cross-correlate it with other information, such as location information and calls, is certainly a step forward in providing credible evidence for corroboration. This evidence on its own really should not be seen as an opportunity to look at a single source and to be able to determine the evidence from that. A great worry from our point of view is that within a private network it is very difficult to pick off individuals, so anything that can be added to that certainly helps.

Erka Koivunen: I am an engineer by background. To me, there is only the content, the payload, that we are protecting and then the metadata that describes who was communicating and where the communication was going to. There is other related information such as what type of encryption and network protocol was being used. I read with great interest about the events data, entity data and related communications data which this Bill would recognise, but to me it sounds as though you would need to tap into the network, take all the data and then start peeling the communications so that you could drop the actual payload. Afterwards, when you start dissecting the communications data for law enforcement and intelligence purposes, these terms become relevant, but when the data is acquired it does not matter how.

Eric King: In the interests of time, I will say no more than what I said previously in answer to Andrew Murrison, other than to agree with the best analysis that I have read on this point. It is by Graham Smith, who I believe you have had before you already. I know that he submitted something to the Science and Technology Committee on exactly this question. It was a masterful dissection of a complicated set of questions. I will not attempt to explain it here for fear of embarrassing myself or doing his argument an injustice, but it is one that should be rated very highly.

Q212 Lord Butler of Brockwell: I think you have partially answered this question already, but I will just ask whether you have anything to add. How clear is the definition of internet connection records in the Bill, and is it practicable to get a clear definition that will meet the purposes of resolving the IP identity?

Eric King: The first thing that needs to be remembered about internet connection records is that it is not a term that exists naturally, unlike phone billing records. It is an invented set of ideas. As a result, the first thing we should do before putting new authorities in place is wait to see the outcome of the IP resolution efforts that were made earlier this year with the Anti-terrorism, Crime and Security Act. It is still only months since that Act was passed. Its goal was to provide for IP resolution, which is the same stated goal in this Bill. It is unclear to me why we have not waited to see the fruits of that, to see where the gaps may or may not be, and to learn lessons where we can. The closest I have seen to any state attempting this elsewhere is in Denmark, which had a similar scheme over recent years but stopped it—two years ago, I believe—after it was found to be ineffective. With that, my caution would be to say that we should learn that lesson and wait for any lessons that we can learn from the IP resolution measure that was passed earlier this year.

Lord Butler of Brockwell: Going back to our earlier discussion, is not the answer that this is just a power, so the Home Office could wait for some time before it exercised it? Would you have any objection to this power being in the Bill?

Eric King: I think I would. I am not sure that the blanket retention of communications is a proportionate activity per se. In the Digital Rights Ireland case last year, the CJEU struck down a similar authority for telephone records. My position at the moment is that we should not be legislating at all in this area until cases that are going up to the CJEU are resolved, for fear of us all wasting quite a lot of our time and having to re-amend and re-adapt the law, particularly given that we could be waiting to see how the Anti-terrorism, Crime and Security Act is implemented. I think we should hold back in this area and not include it in the Bill at all.

Lord Butler of Brockwell: Do your colleagues have anything to add on ICRs?

Erka Koivunen: I would like to continue with a Danish example. I have been told by my old Danish colleagues at DK-CERT that there was an attempt to mandate that all public wi-fi providers should be required to keep session logs of where their users were communicating to. This would include not only telecommunications operators but cafés, conference halls and airports. I used to work for a telecommunications provider and we used to call these cafés hobbyists. These hobbyists would be required to gather sensitive information about who their users were communicating with and they would need to retain that information and have it available whenever law enforcement requested it. To a cybersecurity

professional, that spells disaster. It is a disaster waiting to happen. Each and every store of this kind of information would be a target for computer intrusions by criminals and foreign intelligence services. One also has to remember that it would be pretty expensive for the service providers to start collecting that. In Denmark, in the end, that is why the so-called hobbyist providers were exempted from that legislation, and eventually that whole law was scrapped.

Professor Bill Buchanan: I go back to my point that proxy systems hide the IP address of the sender. Tunnelling systems hide the content. Tor systems hide the content and the IP addresses of the sender and the destination. VPNs hide the content and the source address. Many people are moving to cloud-based systems: you can run virtual desktops within the cloud. The concept of running things on hardware is going. We are moving towards almost a mainframe-type system. We have a terminal that we connect to the cloud and the cloud exists somewhere else on the internet. Anyone who is even a little bit tech-savvy is able to pick one of those systems and hide their logs. Providers need to think through all the options and collect other information which can then be used to corroborate with the pinpoint of information that you might get from an internet service provider.

Lord Butler of Brockwell: So you would conclude that, in its present form, this is not value for money?

Professor Bill Buchanan: In its present form, from a technical point of view, it can be very difficult to find the information that is actually required from purely internet-based records. There is a whole lot of other information that we leave behind. If we have a mobile phone we can be tracked every time we make a call, and so on. There is a whole lot of other information that could be used alongside the internet record. This is not the catch-all that it could be. Ten years ago it was: you could look at anyone's record. The one company that has the whole record of every little thing we have done on the internet is Google. It has all our information. That is because it is the end point. It is the place that you go to and it will see all the information. Unfortunately, that jurisdiction is not inside the borders of this country.

Q213 The Chairman: Clauses 51 to 53 of this very long Bill talk about a request filter. What are your views on that?

Eric King: If I may, I would like to get back to the Committee on that, once I have some questions clarified by the Home Office about the exact scope of what it intends. My starting point is that it permits the same sort of data-mining at a scale that so far only our intelligence and security agencies have been undertaking, and provides that to the police, but in the name of a safeguard. Regrettably, a more detailed analysis requires more information but I will be very happy to provide the Committee with that once it is available.

The Chairman: Would you like to comment on that?

Professor Bill Buchanan: It is certainly a good way forward. Some sort of definition of the search terms that would be used would protect us from a large-scale data breach. The last thing we need is for all the information from an ISP to be leaked because a log was allowed to be taken of its site. The logs should be kept in a trusted environment and the access to them should be locked down to IP addresses and to biometrics if possible. Because they

are probably among the most sensitive logs that we have, if we make sure that the requests made actually match what has been collected, we can make sure that a summary record is given to law enforcement, not the full record. Systems are easily breached. You can take data quite easily from them. It is very difficult to protect them. An abstraction around a request filter is a good way forward.

Q214 Lord Strasburger: Is it reasonable and practicable to require communications service providers to remove the electronic protections from their data when providing it to law enforcement agencies and the security and intelligence services?

Eric King: This issue has taken on increased importance due to how it seems that the Home Office wishes to apply it in future. If it intends to use it to force companies such as Apple to remove encryption or to re-architect their systems to provide a backdoor, that would be wholly inappropriate. It would provide a lesser degree of security for us all. The Home Office needs to answer many more questions as to how it intends to use this authority. If the companies' public statements on this issue are to be believed, we should all be concerned.

Erka Koivunen: From a technical point of view, if the telecommunications operator which has been served this kind of information request is able to remove those protections, which are typically provided through encryption, of course it would make sense for these protections to be removed to enable the law enforcement and intelligence agencies to make any use of the data that they receive. However, echoing what Mr King said, there are many stakeholders in these communications service providers. Some of these providers have designed their systems specifically to employ end-to-end encryption, where the service provider is not in a position to open up the encryption. The encryption goes through the service provider's systems so that even the provider is not able to see through it. The way I am reading the Bill, it would actually ban the use of strong cryptography and strong encryption and would essentially weaken our ability to use secure online services.

Going back to the question of future-proofing, as a company that provides systems where we potentially are not able to decrypt the traffic that we pass—

Lord Strasburger: Sorry, did you say "are" or "are not"?

Erka Koivunen: We provide services that we would not be able to decrypt ourselves. We are not sure whether the Bill would concern us—whether we would be compelled to redesign our systems. I imagine that Apple will be reading the Bill with a similar sentiment. I think that it would refuse to redesign its systems in a fashion that would open up and weaken the encryption. So the Bill has some problems in the way it has been written.

Professor Bill Buchanan: Cryptography and the methods that we use in cryptography are almost perfect. Unfortunately, it is the humans who implement it who are flawed. The humans who implement security, too, are often fairly flawed in their approaches. If you ask most people whether they trust that their ISP's or CSP's security is robust enough to handle secure information such as this, I think the majority would say no, especially after the TalkTalk hack. I have many examples of where they use weak passwords and so on. If we have now got to the point where our banks can be trusted with data because of the CBEST standards and can be put to the onerous task of protecting records such as this to provide

lots of different levels of access, then the ISPs and CSPs have to up their game many times over. They have typically grown from telecoms providers and have been merged from lots of little companies to provide big, heterogeneous types of organisations that are difficult to control.

The only way is with multifactor authentication. The idea that you can open up some data or a log with a single key or a single password has gone. The controls and the proving of identify is key to providing access to the data. The data should never appear offsite at all. The only way you should be able to access the data is by remote access and only through a portal. If we were to risk the opportunity of downloading a whole aggregated log on to a machine with a single encryption key then we really are opening a can of worms. CSPs and ISPs need to be thinking about access. Certainly there should be some biometrics in there—fingerprint recognition at least, along with geolocation, so that only certain locations would be allowed access to it. A mobile phone, through out of band identity methods, is also a good way. You really must wonder, "If my password is changed by my mother's maiden name on my ISP, anyone can find out my mother's maiden name fairly simply from an internet search". If that is the level that ISPs and CSPs are now at, they need to recruit a whole lot of security engineers, architects, cloud engineers and so on. They need proper investment because this will be a massive task. The banks are soaking up all of our graduates to work in these types of environments. The next wave is that if the UK cannot produce enough cybersecurity specialists, where will we get all these new specialists? The country needs to think ahead and, I hope, invest with the ISPs or CSPs to make sure that they protect our data.

Lord Strasburger: What are the risks and benefits of allowing law enforcement and the agencies to undertake equipment interference? I mean both types of equipment interference, targeted and bulk.

Eric King: On the law enforcement side, the most powerful argument I have heard for preventing law enforcement having access to equipment interference was from the Suzy Lamplugh Trust earlier: the powers they are currently provided with are not being used to their fullest. Given the incredible intrusiveness that equipment interference could provide law enforcement, we should treat it with extraordinary scepticism. One of the issues at the front of my mind and which I have not had an answer from police or the Home Office on is how we will get around the issue that, by deploying equipment interference—what the agencies sometimes call "computer network exploitation"—we will not damage evidence that the police would later wish to seize and rely on in court. It seems that it would be incredibly counterproductive to be providing an authority in this manner that, in some circumstances, could result in criminals getting off the hook. Until I hear a compelling answer from the Home Office on that point I am not sure that we should move forward with that aspect.

In the intelligence domain it is far more severe. I struggle to understand exactly what the Government have in mind by bulk equipment interference. Every single scenario that I can conjure up seems to be within the scope of what are the not very targeted but nevertheless called targeted equipment interference powers that are there. That is because it provides them with thematic warrantry or even hacking by location. That by itself is very broad. We need to understand that, by undertaking interference, our agencies threaten British

cybersecurity. They regularly hack companies in Europe and elsewhere that are not a national security threat in and of themselves. The employees of those companies are not suspected of any serious crime or criminal wrongdoing, but these companies are being attacked to allow GCHQ and other agencies to undertake further attacks. In recent years, we found out that GCHQ hacked Belgium's largest telecoms provider, Belgacom. It has also hacked Deutsche Telekom, Seagle, Stella—the list goes on and on. In doing so, they are painting targets on British companies' backs in exactly the same way and legitimising these kinds of attacks. By attacking using vulnerabilities in networks and systems that they have acquired themselves but are refusing to tell the world about so that those companies can protect themselves, they reduce the security that we collectively experience. The stockpiling of these vulnerabilities in zero-days is not considered in the Bill. Policies need to be very clearly set out about it before any consideration is made of the powers. As it stands, our recommendation to the Committee is that bulk equipment interference should be absolutely prohibited. There seems to be no good reason why such a thing could be undertaken. Should equipment interference be permitted at all, I point the Committee to the recommendations made by Privacy International and the Open Rights Group as a result of the draft equipment code of practice introduced earlier this year in response to recommendations.

Lord Butler of Brockwell: May I ask one short supplementary on that? You say that we are putting British companies at risk by pinning a target on their backs. Foreign interceptors are not going to intercept British companies just by way of revenge, are they? They will do it anyway if they want to.

Eric King: I would hope not. Nevertheless, by using vulnerabilities and imagining that we are the only state that has discovered them we allow British companies to continue to be exposed to those threats. Instead, when British agencies find a vulnerability in networks, their presumptive position should be to disclose that to the appropriate vendor so that all companies can benefit from that security. Instead, by keeping them and using that as part of attacks, we first raise a flag, so that when those attacks are eventually discovered others will use that same attack here in the United Kingdom. Secondly, we are preventing them from being able to defend against attacks that we could be assisting them in preventing in the first instance.

The Chairman: We are getting very close on time now.

Erka Koivunen: The term "equipment interference" is pretty elegant. When I was learning information security at school we used "exploitation", "vulnerabilities" and "attacks" to describe the same things. There was no discussion of vulnerabilities or attempts to let the vendors of software products know about them. Equipment interference also refers to the deliberate introduction of those vulnerabilities and backdoors in products. In recent days, we learnt that Juniper, a big provider of core networking components that the internet is being built on, found backdoors and means to weaken encryption in its systems. This backdoor was in its code for at least two years. This was probably of use to some intelligence organisations' operations around the world. However, the UK networks, the Finnish telecommunication providers' core networks and the corporations' networks are being built by the exact same systems. They have been vulnerable to this type of exploitation for two years already and are not rushing to patch their systems. Cisco Systems

had a similar case a couple of years ago that was not publicly discussed. There are many systems where it has been suspected that vendors have been compelled to introduce backdoors of this nature to deliberately weaken cybersecurity protections in favour of some intelligence organisations. I see this as a threat to civilian society's ability to conduct business online, and to e-government processes. When we cannot trust our information-processing infrastructure, we tend to avoid using it to conduct business.

The Chairman: Very briefly, Professor.

Professor Bill Buchanan: My view is that virtually everything is possible and it should be based on a risk-based approach. If something is high-risk these things should actually happen and we should be looking at exploiting vulnerabilities. As long as there is a reason for doing it and it is documented and audited, really anything is possible from a technical point of view.

The Chairman: Thank you very much indeed. Mr Warman, you have a final question before we move on to the next session?

Q215 Matt Warman: I should declare that my wife is a student at Queen Mary, but not one of yours so do not worry. If we look round the world, how does this compare to international legislation that is coming forward or is currently in force?

Professor Bill Buchanan: In France just now the access to public wi-fi is being looked at. In Kazakhstan, of all places, they are looking to implement a digital certificate where you cannot connect to a secure channel unless you use the Kazakhstan certificate. Unfortunately, the problem with that is that none of the cloud providers trust that certificate, which means that it could decimate their business and the social aspects. It has been done with the aim of improving privacy but there may also be a political agenda. It has also been shown that general certificates can be hacked. It happened when Iranian hackers got access to the DigiNotar certificate, which was a Dutch certificate, and managed to hack 300,000 users on Google and listen to their communications. Most countries are now looking at the inability to view logs. Few countries have been able to get the balance right.

Erka Koivunen: As a matter of fact, I am participating in the reform of the Finnish intelligence legislation and there are discussions about targeted equipment interference, using the terminology in this Bill. There is a pretty wide consensus that attacking foreign military installations will be something that we will see parliamentary consensus on next year, when it goes to parliament in Finland. The intelligence services in Finland have already publicly stated that they are refraining from demanding backdoors and the weakening of encryption while they seek a new mandate.

Eric King: There are lots of comparisons we could look to but we should focus on the United States as a country that we share a very similar capability with; under the Five Eyes Alliance, we also have much the same approach to issues. Over the past two years in the United States, reforms have been made to curtail NSA capability. There is one power in particular that I bring the Committee's attention to, and that is to do with bulk communications data acquisition. This is what was avowed by the Home Secretary to the Commons when introducing the Bill. While we have very little information about how this is used in the UK,

in the United States this was on the front page of most newspapers. Very helpfully, two independent bodies that had access to classified material were able to look at the programme and consider it in detail. The President's Review Group on Intelligence and Communications concluded that the use of this was not essential to preventing attacks. Similarly, the Privacy and Civil Liberties Oversight Board concluded that, "we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot". This is a power that there have been two detailed reviews on in the United States and that they have decided to end. Indeed, it was just a few weeks ago that that programme was brought to a close but here the Bill is attempting to place it on a statutory footing for the very first time.

Matt Warman: That is not a technical point—if our agencies were to say that they thought it was necessary for national security, there is not a technical argument for making the observation that for political purposes or whatever they have made a different decision in a different country?

Eric King: In the country in which an operational case was made, that could be scrutinised by a series of very senior experts—who in many circumstances were very close to the intelligence community—who had access to classified material, who looked in detail at the operational case and found it lacking. My presumption is that the Committee should take the same approach until such a time in which the security services provide a public rebuttal and can show that the operational case is somehow different from the one that was so carefully scrutinised by so many people in the United States.

The Chairman: Thank you very much, all three of you, for a very interesting session, particularly Erka for coming a long way at relatively short notice. We wish you a very happy Christmas.

Christopher Graham, Information Commissioner (QQ 224-233)

Evidence heard in public Questions 224-233

Oral Evidence

Taken before the Joint Committee

on Wednesday 6 January 2016

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins, Suella Fernandes MP, David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Bishop of Chester, Lord Hart of Chilton, and Lord Strasburger.

Witness: **Christopher Graham**, Information Commissioner, gave evidence.

Q224 **The Chairman**: Welcome, Mr Graham, and thank you for coming along to talk to us this afternoon, so soon after the new year, when we are just starting up politically. As you know, this is an extremely important Bill, which is going through both Houses. We have been charged with the task of pre-legislative scrutiny. You undoubtedly have significant views on the issues that are in front of Parliament. I am going to kick off, if that is okay, with a rather general question to you. If you wish to add some comments more generally, we would be delighted to hear them. Thank you again for coming along. My question is: do you think that the draft Bill is actually necessary, from your point of view, and does it strike a balance between privacy and security—the age-old balance between those two things?

Christopher Graham: Good afternoon, Lord Chairman, and thank you for inviting me to contribute to your deliberations. I know that you are having to work very fast on a very complicated Bill; I counted nine parts, 202 clauses and nine schedules and I think that you have to report back to Parliament very speedily.

To answer your question, some legislation is clearly necessary, because the previous legislation was struck down by the courts. Indeed, the fundamental question about necessity and proportionality is still before the Court of Justice of the European Union. Nevertheless, following the reports from David Anderson and RUSI, suggestions were made for making much clearer and much more explicit what the proposals for the use of data are and what the procedures and safeguards should be. I suppose that this Bill is a response to that.

It is very difficult to judge whether the Bill gets the balance right between security and privacy. The one thing that we do not have in the voluminous material that has been put before you is any real evidence, as opposed to the occasional anecdote, on the utility of the information that is sought. The Bill proposes that data can be required to be retained for 12 months, but there is no particular explanation of why 12 months rather than six months or 18 months is desirable, because there is no indication of the use that such information is being put to over many months and years in the normal way of dealing with serious crime and terrorism.

All that I would say as Information Commissioner, in answer to that point, is that Parliament needs to see this in the context of the way the digital world works. Whatever we do, we are all leaving a trail of information, but we also have rights, under the data protection directive and the Data Protection Act, to have our privacy respected. There needs to be a balance between the common interest in security and the individual interest certainly, although I would also say the common interest in privacy and an acceptance by Parliament that data protection is a fundamental right under the Charter of Fundamental Rights of the European Union. I do not think that it is a question of just signing a blank cheque. I would be very much in favour of Parliament continuing to stay with this issue and, after the legislation is passed, as I suppose it will be, making sure that it returns to the issue time and again to make sure that the information that is being retained and exploited is being used properly and that the use is proportionate, needful and helpful.

Q225 The Chairman: Thank you. In your written evidence you said something that the Committee found very interesting about the question of a possible sunset clause in the legislation. Perhaps you could expand a little on your views on that.

Christopher Graham: This develops the point that I was just making—the proof of the pudding, Lord Chairman. It is asserted that this information is very important for the prevention and detection of crime and terrorism. I think that it would be sensible and wise for Parliament to review from time to time how it is working in practice. What use is being made of this great mass of data that will be required to be retained by communications service providers? Did it actually contribute? There is a huge risk, with all that information being retained that otherwise would not be, that that information could be exploited by bad actors, so there are security challenges for communications service providers. Parliament would need to be convinced that the case that had been made was working out in practice. After all, Parliament renewed the Prevention of Terrorism Act year by year, so I cannot see why we should not have a similar arrangement for something so fundamental as this Bill.

The Chairman: Would you see that as being an annual review or a bit longer than that?

Christopher Graham: Well, Parliament managed to do an annual review of the Prevention of Terrorism Act and took it in its stride. That was when life was a little simpler. We have to bear in mind that if we are saying to communications service providers, "We want you to retain everything for a year and then, under a system of warrants, we reserve the right to look at it", we are building up a risk around data security and privacy. Parliament has to be pretty sure that that remains justified and that the arrangements remain secure. One way of doing that is to have a sort of rolling sunset arrangement.

Q226 Lord Strasburger: Good afternoon. One sentence in your written submission caught my eyes. In paragraph 7, you say, "there is an increasing danger that we are living in a society where few aspects of our daily private lives are beyond the reach of the state. This poses a real and increasing risk that the relationship between the citizen and the state is changed irreversibly and for the worse". What did you mean by that?

Christopher Graham: What I meant was that simply by the fact that we are all doing business, social interaction and communications digitally, wherever we go and whatever we know, like it or not, we leave a digital trail. The challenge for a data protection

framework is to make sure that that remains private where it should be private or, if it is accessed and shared, it is accessed and shared within a regime of data protection where all the rules are agreed. What I am not prepared to sign up to is the suggestion that willy-nilly the state ultimately always has a right to access all that stuff, just because (a) it can and (b) "Salus populi est suprema lex", and all that. The case has to be made constantly for the necessity and proportionality of anything that invades our privacy, whether it is a commercial invasion, whether it is by state agencies, whether it is information sharing within the health service or whether it is information to keep us all safe and secure in the face of terrorist threats. I am not pretending that that challenge is not there; I am just saying that we have always to be clear that the rules under which that information is accessed have integrity and are closely followed. The fact that the state and commercial entities can have access, physically, to this material is obvious; the question is under what regime they should be allowed access in a good cause.

Q227 **Mr David Hanson:** In your written evidence—and you have touched on it again verbally today—you indicated that you think there is little justification being advanced for the 12-month retention period. Ultimately, do you think that the 12-month retention period is correct or not?

Christopher Graham: When I say that little justification has been advanced, I mean that those who are putting forward this Bill are not explaining what 12 months is about—why 12 months? If you are going to say, "We reserve the right to invade your privacy, and by the way this material has to be retained for 12 months", you have to make the case for that. Nowhere in the Bill or supporting memoranda have I seen the argument for 12 months. It is not for me to say that I think 12 months is wrong or right or that some other figure is appropriate because I am not the one seeking the powers; I am not the one who knows what we want to do with the information; I am not the one who knows how the information has been used. I am realistic; I understand that there has to be some care with which the facts are bruited abroad but nevertheless, nowhere in this 296-page package is the case actually made for 12 months.

Mr David Hanson: We have received evidence from police and other agencies that there are long, drawn-out investigations where serious crimes are potentially being committed, or have been committed, where the 12-month retention period is required. If that case were made by the Home Secretary and/or the agencies, you have no objection in principle to the 12-month period as opposed to a shorter or longer period?

Christopher Graham: I do not know what advice you have seen; as I say, it is not in the 296-page pack. But I would be a little wary if there was one anecdote—one case, I apologise—where information that was 12 months old was useful. I would still take some persuading that that justified the retention, potentially, of everybody's everything for 12 months, just in case.

Q228 **Dr Andrew Murrison:** Good afternoon. In your evidence you suggest that there might be a stronger role for the Information Commissioner in auditing communication data. I would be interested to know what you mean by auditing and what exactly you would be checking up on. Would it be the kinds of data sets that have been gathered or the way that they are stored and managed, or the way that they are used by the authorities?

Christopher Graham: To be clear, I am talking about the role of the Information Commissioner under this Bill being very similar to the role that we have under DRIPA and the Data Retention Regulations, which is not to make judgments about whether or not information should have been used in the way that it was used but based simply on the data protection principles of making sure that information that is retained which otherwise would not be is retained securely, is not inappropriately accessed by people who have no business to see it, is not leaked and does not go AWOL, and that it is also securely deleted at the end of the specified period. My good practice team and my expert auditors are engaged in that process and I imagine that under these proposals they would continue with that sort of work.

To do that, I could do with a few improvements to the Bill, if I may. I have obligations as the Information Commissioner under the existing legislation to audit communications service providers and to make sure that information is secure and is appropriately deleted. But the communications service providers do not seem to have any very specific obligation to co-operate with me. I am not saying that they do not co-operate but it takes an awfully long time to get in to see the communications service providers. I would like to see that not left to codes of practice but in the Bill.

I think it would also be a reassurance to those communications service providers if they were absolutely confident regarding the same obligations that my staff have under the Data Protection Act to keep secure the information that we receive in the course of an investigation; Section 59 of the Data Protection Act carries a criminal sanction if I or any of my staff abuse our position. That should be explicitly extended to the obligations on the communications service providers under this legislation so that they have the confidence that any information they share with me and my staff will be respected under pain of criminal sanction. I make this point because we are wasting an awful lot of time sending auditors on to sites to spend three days reading up all the material; if we could see it in advance, we could prepare and just turn up and do an audit based on the questions that arise from the material. Those are very practical points which would make the job of the Information Commissioner a lot easier and probably the ICO easier to deal with for the communications service providers.

But you ask about the use of the materials retained, and that is just not my territory. That is not what I am asked to do. You have had evidence from the distinguished commissioners who labour in that particular vineyard. I think I said in my initial remarks that I cannot make that assessment. I just do not know how that information is used and whether it is used appropriately. If Parliament is relying on me to answer those hard questions, you need a better structure in place for dealing with it, which is why I suggested post-legislative scrutiny, sunset clauses, and so on.

Dr Andrew Murrison: Do you think that those who drafted the Bill struggled with putting obligations on CSPs which they could not then enforce? The last thing we want is a law that is unenforceable and could be waived by authorities outwith the territory of the United Kingdom, for example.

Christopher Graham: I think that all the communications service providers want to co-operate as best they can. I have seen the suggestion that some of them are worried that if they accept the principle of extraterritoriality in the case of the United Kingdom, they might

be required to do the same for the Chinese or the North Koreans. I do not detect any reluctance to co-operate sensibly. But the fact is that under the present legislation—DRIPA—my statutory obligation to carry out the audits of security and timely deletion is seen by communications service providers as just another regulator doing what regulators do, and I need that more specific legal power to make sure that we crack on with things in a business-like way.

Q229 Stuart C McDonald: Mr Graham, you have already referred several times to the importance of the security of retained data. Based on your experience of auditing communications service providers' retained data, how much faith can we and the public at large have in the security arrangements that they have in place for retained data?

Christopher Graham: We have been charged with that responsibility under DRIPA only over the past couple of years or so. We have managed to get round the major communications service providers in the UK. I would have liked to have been able to do it faster. As I said, perhaps the communications service providers did not have the same sense of urgency that we had, but nevertheless we have got round the communications service providers. We have not found things that shocked us, I will put it that way. Under this legislation it will be very important to continue to make sure that arrangements are in place for the secure retention of data. We had concerns about data perhaps being housed with other data that would be accessed in the normal course of business and it probably was not a good idea to have those two data sets held side by side. We are very keen to engage with the communications service providers to make this system work.

Stuart C McDonald: Are the service providers quite co-operative in resolving that sort of issue if you raise it with them?

Christopher Graham: Yes, our problem has really been a scheduling one; unless I have the statutory power to say, "I am sorry, I am not asking, I am telling: I am coming", the answer will always be, "It is not really convenient. We will see you in three months' time. Oh dear, that is not convenient either. We will see you in another three months' time", and so on. I want the explicit power in the Bill to be able to go in and audit communications service providers in the same way that I can with government departments or health service bodies. This is really important. If you are saying that the nation's communications data is going to be held under some circumstances or even most circumstances, where it otherwise would not be, the regulator has to be given the powers to make sure that that is actually being done properly: that the information is being held securely and when it is dealt with it is gone.

Stuart C McDonald: From what you said, you have not had the opportunity yet to look at some of the smaller service providers and the security of the information that they retain.

Christopher Graham: Yes, it has been fairly slow work but we will continue with that whether or not the Bill goes through.

Stuart C McDonald: You have spoken about co-operation a couple of times. I sense that it is not so much a complete lack of co-operation but just a lack of priority or urgency on their part.

Christopher Graham: Yes, "lack of priority or urgency" is a fair way to characterise it.

Stuart C McDonald: What involvement do you have with overseas-based service providers and what is your relationship like with them?

Christopher Graham: We have a good relationship. Some of the big players, of course, are based elsewhere. But as the UK data protection authority, we are dealing with these players all the time. We usually have a pretty good working relationship with them and we will see how this legislation works out.

Stuart C McDonald: So you do not notice a difference between overseas-based providers and UK-based providers? Is there roughly the same level of co-operation?

Christopher Graham: The same level of co-operation, I would say, yes.

Stuart C McDonald: You also have experience of auditing the information-handling practices of police forces. Again, how much faith can we have in the security of the information and data that they retain?

Christopher Graham: We have been auditing police forces for years under the Data Protection Act and the Privacy and Electronic Communications Regulations. We have audited 40 forces. Again, this is a consensual audit—I do not have the power of mandatory audit—but again we have not had a single audit where the conclusion has been "very limited assurance". Breaking down those 40, we have had two that came in at "high assurance", 24 that came in at "reasonable assurance", and 14 that came in at "limited assurance". Where it is limited assurance, we have a checklist of the things we want the force to do before we go and see it again. The police service is very much engaged with the data protection and security issue. We are talking to them all the time and working with the national police improvement people—formerly, ACPO—and I am reasonably confident that we have a good working relationship with the police. Again, what I cannot judge is what use the police are making of retained material.

Stuart C McDonald: Sure. Indeed, there was a news story just a couple of days ago about the completely inappropriate use of retained material by one or two rogue officers. There has to be a limit to what you can achieve. You can never do anything more than make sure that appropriate systems are in place. You cannot ensure that an individual officer is not going to go rogue, as it were. Can systems be put in place to try to stop that sort of access to information?

Christopher Graham: There is the criminal sanction in Section 55 of the Data Protection Act. I might wish that Parliament could persuade Ministers to activate a greater deterrent penalty; at the moment, it is a fine-only regime. Of course, Parliament passed legislation to enable the possibility of a prison sentence but it has never been commenced. That is something the Committee could recommend. We do act when individual officers go rogue. It merely underlines the point that when you require communications service providers to retain a massive collection of data for a year, it creates a risk. It is there. People may do stupid things with it. The Committee should not concentrate simply on whether or not use by the forces of law and order is appropriate and appropriately warranted; it is also just a whole pile of stuff that can get lost or inappropriately accessed from a criminal point of view and so on. Because that risk is created by the legislation, you have to have some very

powerful safeguards to make sure that the legislation is reviewed regularly, that it is being used for what it is meant to be used for, that it does what it says on the tin, and so on.

Stuart C McDonald: Finally, do you have involvement in auditing the information-handling practices of the intelligence agencies? If so, what faith should we have in the security of the information that they retain?

Christopher Graham: No, I am not invited to that particular party.

Q230 Suella Fernandes: Good afternoon. I have a simple question, if there is such a thing. There is an issue around when privacy rights are engaged and I wanted to get your perspective on when you think those rights arise. Does an intrusion occur when information has been read? Is it when it has been analysed or subjected to automated filtering or to human examination? What is your perspective?

Christopher Graham: The risks and the rights arise at the point of collection. It is a fundamental data-protection principle under the directive from which the Data Protection Act arises that information is not retained for longer than is necessary. If you create the requirement for information to be retained, that calls into question the obligation under the seventh principle, that personal information must be secure. The very first principle – that personal information must be fairly and lawfully processed – arises when the profiling of individuals takes place based on the information that has been retained, and decisions are taken about individuals that may be to their disadvantage that have nothing to do with law and order or security but are just about treating people differently because of information that you have been able to get hold of. So I would not subscribe to the view that it is a question only of deciding on the proportionality and necessity of looking at particular pieces of information because we have reason to believe that so and so is up to no good. I do not oppose that at all. I am just saying that information rights are impacted and a risk is created simply by the amassing of this huge amount of personal information, which may or may not be needed for the purposes that it was originally collected for.

Q231 Lord Hart of Chilton: Good afternoon, Mr Graham. You say in your written evidence: "Examples of the need for bulk personal data set warrants are not persuasive since equivalent provisions already exist in statute. The established approach could be used for data sets of concern. Consideration should be given to exempting certain data sets involving sensitive personal data, such as those, for example, relating to health data". How would the provisions of the draft Bill alter the range of these data sets, and how would you like to see the Bill amended to provide the audit arrangements that you say are necessary?

Christopher Graham: The point that I was making was that in the Explanatory Memorandum—the guide to powers and safeguards—the authors of the Bill have chosen some very inapt examples of the sorts of bulk data sets they want to access for reasons of law and order, by giving the telephone directory and the electoral register as the two examples. This is bizarre, because that information is already available. Explicitly, legislation was amended to make sure that that information is available to the security services. It does not require this Bill to provide that. That begs the question of what are these data sets that are so necessary, and we are not told, which then begs the question that if the authorities are not going to tell us what data sets they are going to be accessing, are they prepared to say what data sets they would not be prepared to access?

There is very great public concern about various initiatives in the health sector around the care.data project. Patients were very concerned that their most personal and most sensitive information was going to be uploaded into a health service information centre and then shared around rather freely with the insurance companies and heaven knows what. People were very concerned about that. That scheme has now been rethought and that is very good news. But are we being invited to give a blank cheque to the authorities to access everyone's most sensitive health data? I suspect not, but it does not say that in either the legislation or the guide to powers and safeguards. It seems to me that they picked a silly example, because you can already access the electoral register and the phone book, but there is some reticence about talking about what would be off-limits.

Lord Hart of Chilton: Earlier, you gave some examples of how you would like amendments to be made. Do you have any amendments you would like to be made here?

Christopher Graham: I would probably stick to the job that I am charged with, which is inviting the Committee to consider specific amendments to those statutory obligations I am under about the auditing work under the Bill that we are specifically asked to do. I have two roles here: one is to make the general point about the balance between security and privacy, which of course has also been made by others in evidence to you; the second is dealing with the specific powers and duties of the Information Commissioner under this legislation relating to the auditing of retention and deletion by communications service providers. I think I will probably stick to that, if I may.

Q232 **The Chairman:** It has been argued that the revelation of details of further data sets could damage the work of the security services. Do you think they have a point?

Christopher Graham: That is the eternal dilemma of this subject. I have been Information Commissioner for six and a half years, and before I even took up the post I was being approached by the Home Secretary to understand the absolute importance of what was then going to be the communications data Bill. It is very difficult to get the rules right, and I understand that security services and the police find it difficult to be explicit, because it gives the game away to bad actors. The trouble is that the Anderson report last year and the RUSI report called for an end to obfuscation and secrecy, and said that we must have transparency to win public confidence. The Home Office should probably be more forthcoming about what it is talking about here. We seem to be a bit betwixt and between—more transparent than we were, but not quite transparent enough to win the argument.

Q233 **Bishop of Chester:** It is good to see you in this context. It falls to the bishop, for some reason, to talk about oversight and how it works in these contexts. You said that the new IP commissioner "must be independent and inspire public confidence". Do you think the draft Bill is framed in a way that will promote that?

Christopher Graham: Well, clearly there is a lot riding on the new commissioner. The way in which the commissioner is appointed will be key. As a commissioner myself, the resources that the commissioner has to do the job will also be very important. You can have high-sounding powers and responsibilities but if you do not have the resources and people to carry them out, that will be a complication. We have done a lot of work at the Information Commissioner's office working with the various Home Office commissioners

to try and make it clearer to the outside world how the regulatory framework goes. At my initiative, the various commissioners published a road map of surveillance, so that individuals could see who was doing what. We work very closely together. We are working on a memorandum of understanding with the Interception of Communications Commissioner, in particular on the reporting obligations for communications service providers to make sure that they need tell us only once, in effect, and then it is up to the two commissioners' offices to work together to make sure that the right people get to know what they said.

Primarily, in my experience, commissioners are judged by the way in which they perform. Obviously, commissioners will be expected to appear before parliamentary Committees and so forth. A commissioner will be expected to report regularly. Clearly, the Interception of Communications Commissioner's office is an exemplar of how that should be done at the moment. Fundamentally, is Parliament or the Home Office going to vote the funds to enable the new commissioner to do a proper job?

Bishop of Chester: What is it about your present role that you think really promotes your own sense of independence as the Information Commissioner, and the public confidence that there clearly needs to be in your role, too? What is the key thing that supports those features of your role which should potentially transfer to the new role?

Christopher Graham: I am tempted to say to the Bishop of Chester, "Not being based in London", but it might be fanciful to think that this commissioner will be based in Wilmslow or anywhere similar. It is not a trivial point: there is some advantage in being just a little bit distant from the centres of power and influence in Westminster. Otherwise, it is a question of having the resources to do the job. I am funded by the levy that all data controllers pay. Many £35s add up to the best part of £18 million or £19 million, so my office is very well resourced. I hope the new commissioner will be similarly resourced, at least in the sense of adequately, though I suspect that would more likely be by grant in aid from the Home Office. This is an important area. It must be properly funded.

Bishop of Chester: We have been discussing how the funding regime would work for this. Are you content with how your role will relate to the new commissioner's? Do you feel comfortable with how that would be set up?

Christopher Graham: We have to make it work. As I said, it was at my initiative that I got together with all the Home Office commissioners and also the Surveillance Camera Commissioner and the Biometrics Commissioner. We had very regular meetings and produced that road map. We are working on a memorandum of understanding to make sure that we do not cause aggravation to communications service providers by asking the same set of questions twice. It is all in the co-ordination. I do not think that it requires a culling of commissioners—though I would say that—but co-operation between them, certainly.

Bishop of Chester: So are you satisfied with how it is set up to relate to your office, broadly?

Christopher Graham: Yes, we will do our little bit, but it is a little bit of the whole surveillance and security piece, which is a little bit of the whole data protection universe. That is what we are concerned with.

Bishop of Chester: One of the issues for independence is how the roles of authorising interception and overseeing what has been done relate to each other. There have been some suggestions that the commissioners could be like people who mark their own homework: that the same body will, as it were, both authorise warrants and exercise an oversight of that process. Is there a case for greater separation somehow between those two roles with the IP commissioners?

> ***Christopher Graham***: On reading the transcript of the session on 2 December, when you asked that question, I was rather sympathetic to the point you made about the nature of a double lock. It did not feel much like a double lock to me, more like a conflict of interest.

Bishop of Chester: Should it be a triple lock—in other words, by separating the oversight role from the authorising role?

> ***Christopher Graham***: I hesitate to go there. David Anderson originally suggested the clear involvement of the judiciary in the authorisation. My reading of his evidence at the 2 December session was that he seemed quite happy with what had been proposed. I just do not know; all that I am saying is that if, in my office, I had responsibility for one set of people authorising something and another set of people deciding whether they should have authorised it, I would find that slightly odd.

The Chairman: Mr Graham, thank you very much indeed: that was an extremely useful and informative session. Thank you for coming along.

HMRC (QQ 26-38)

Evidence heard in public Questions 26-38

Oral Evidence

Taken before the Joint Committee

on Monday 30 November 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Bishop of Chester, Lord Hart of Chilton, and Lord Strasburger.

Witness: **Simon York**, Director of the Fraud Investigation Service, HMRC, gave evidence.

Q26 **The Chairman:** My apologies for the late running of the earlier session. This was a consequence of Divisions in the House of Lords. You are very welcome. As you know, it is an extremely interesting and important Bill that the Committee is looking at and we very much look forward to the points you have to make to us. Perhaps I could kick off by asking your views on the draft Bill. From your point of view, why have it at all, and how will its proposals affect the work of your own organisations? In that context, which of the powers in the Bill would you regard as new, and which are to be simply consolidated into a new Bill?

Keith Bristow: Thank you Chair. Would you mind if I just made a few opening comments before getting to the specific question? First, thank you very much for seeing us so early. I am representing all senior leaders in law enforcement and policing, because we think this is so important that we need to come before the Committee quickly. Your team has also been very indulgent. I was anxious to bring three senior colleagues who are absolute experts in the breadth of law enforcement.

One of our deputy directors here is Chris Farrimond. He provides many of the law enforcement capabilities to which the draft Bill refers, including lawful interception, CNE and the high-end capabilities provided for the whole of law enforcement. He is a very useful person to have here.

Simon York from HMRC will be able to speak to serious criminality and the taxation system, which again demonstrates the breadth of some of the use that we have to put these capabilities to. Richard Berry is a very experienced police officer in a police force and leads for the National Police Chiefs' Council on communications data. He can speak in some detail about communications data and how it is used across a whole range of policing activities.

Why is this important? Technology has changed the way in which we all lead our lives, which is mostly a good thing for the law-abiding majority. But the reality is that serious and organised criminals in particular, who we target as an agency, also see very significant advantages from technology. That presents us with some very real challenges. The challenges come because the infrastructure of the internet provides some of these people with significant levels of anonymity, which is a challenge for us. The type of data that is

stored and made available to law enforcement does not meet our purposes. The legislation within which we operate is not fit for purpose and was not designed at a time that reflected the age in which we live. The reality is that law enforcement is now experiencing a widening gap. We should remember that law enforcement work is evidential, which is different in many respects from other agencies—the SIA—and it is targeted. The capabilities that we use are brought to protect the public but also to bring people to justice and to discount people and prove alibis.

In the Anderson report, David Anderson identified five purposes that we need for these operational capabilities. Those five purposes remain the same as when we spoke to David Anderson about them. The draft Bill goes a long way towards meeting our operational requirements. We recognise that our requirements are operational and need to be balanced against wider considerations that the Committee, the Government and Parliament in due course will take into account.

Nothing I will say is intended to cut across any of that. We simply want to set out what we need to keep the public safe. One particular concern to which I want to draw your attention—we can put some others in a written submission—relates to internet connection records. The challenge for us is that we believe we need access to all the data that is retained on internet connection records. However, in the draft form of the Bill, that will be limited to three purposes only, which means that data will be retained by communications service providers that we could not request.

As I said, this needs to be balanced against other requirements as well, but it is important to recognise that that limits some of our ability to protect the public and to fight crime.

Lord Butler of Brockwell: Sorry, you said three purposes. What are the three purposes?

Keith Bristow: This is not quite how it is worded in the Bill, but in operational terms one purpose is to resolve IP addresses. It is where a website contains illegal content—or what is called a communications website. For instance, codes of practice may help to refine this and develop our understanding, but it would not include a website where someone could book a rail ticket, which could be hugely important if it related to a missing person. We just need to be clear that data will be retained by service providers to which we cannot request access.

Chairman, you asked specifically about what new powers and new capabilities this Bill would give us. Frankly, it preserves the capabilities that we have always needed, but in a digital age it does not make us more capable of doing things. In operational terms, it brings up to speed what we need to be able to do in a digital age compared to an analogue age. A lot of what we will talk about is comparing what is acceptable to the public, expressed in legislation in the analogue world, how we need to be able to do that in a digital world and how the world has changed.

The Chairman: That is very useful. Thank you very much.

Dr Andrew Murrison: I do not understand this bit about the extra powers that you say you want to have. My understanding is that you could apply for those. Are you specifically talking

about missing persons, because clearly you will be able to get a warrant to get information in relation to serious crime? I am left somewhat confused. Can you clarify it?

Keith Bristow: We cannot request data retained on internet connection records unless it is for the specific purposes that I mentioned. Let me give an example, and Richard is very well qualified to talk about this. If there is a vulnerable missing person—a young person perhaps—and we are concerned about what arrangements they may have put in place to go abroad or to travel, we could not request access to an internet connection record to give us the lead to pursue that point.

Dr Andrew Murrison: Okay, but in relation to a serious crime, as presumably defined by the Serious Crime Act 2007, you would be able to request that data, would you not?

Richard Berry: If I can assist, sir, the major difference with this legislation is that the internet connection records would be retained. If data is retained, for example for business purposes, by a CSP—a communications service provider—then we can apply for that, but forward-facing. The big difference with this Bill is that there will be a retention of those internet connection records and, quite clearly, a process for us to apply for that.

Dr Andrew Murrison: So the information will be retained and you will be able to apply for access to it.

Richard Berry: Yes, but only for the limited categories that Mr Bristow mentioned: so, to resolve an internet protocol address—i.e. to attribute a communication; secondly, to establish whether a person has been using a communications site—Facebook, WhatsApp, those kinds of platforms; and, thirdly, if someone has been accessing illegal content—child abuse imagery or, indeed, terrorist material, that kind of material. There are other policing purposes that we would require access to internet connection records for.

Dr Andrew Murrison: What purposes are those?

Richard Berry: Well, for example; a banking website or, indeed, a travel website. There are case studies that we could furnish the Committee with in writing, if that would be useful, outlining some of those gaps. In a particular case in relation to human trafficking that involves booking flights and the movement of people, we would not be able to obtain that data under the provisions of this Bill. Perhaps I can speak from personal experience having run a large-scale anti-human trafficking operation where 85% of the actionable intelligence came from communications data. That was in the mobile phone era of 2008. We certainly could not repeat that kind of activity now, because the mobile internet communications platforms are where most people now communicate and do those transactions.

Keith Bristow: Might I add two things? Of course the codes of practice, when published, may help us to understand this, but this is our interpretation of the purposes that we can request internet connection records for, and those do not include some of what we will need to access, even though the data is retained.

Dr Andrew Murrison: I am afraid that I am rather confused, because for serious crime—the list is well laid out and, I think, well understood—my understanding is that you would be able to get that information. I am bewildered by what you say. However, there is a question, of

course, about what further cases and crimes you may request information on. I think there would be some resistance to extending the list of serious crimes beyond that given in the 2007 Act, if that is what you are requesting.

Keith Bristow: I am not making any requests; I am setting out the consequence of our understanding, which would allow us to request access to data that has been retained by service providers. You make a point about serious crime, but of course a missing vulnerable person is not a serious crime.

Dr Andrew Murrison: So to cut to the chase, is that your concern?

Keith Bristow: It is one of the concerns, but they are wider than that, because, as we understand it, we can only request data that has been retained by service providers for those three purposes.

The Chairman: So you are telling the Committee that to a certain extent the Bill does not do enough, as far as you are concerned.

Keith Bristow: The question that as law-enforcement professionals we are seeking to answer is: what do we need to protect the public? I am setting out what I believe we need to protect the public, but, as I said in my opening comments, Chair, we absolutely accept that there are wider considerations for this Committee, for Government and for Parliament to consider. I do not think, therefore, that it is for us to set out the operational choices.

The Chairman: You also indicated that any possible codes of conduct that might be constructed might resolve some of these issues.

Keith Bristow: I am not confident that they will resolve them, but they will probably clarify them.

The Chairman: Before Lord Butler asks his question, do any of your colleagues have any comments to make on this?

Richard Berry: Sir, if it would be helpful, the subsection that we are referring to is subsection (4) of Clause 47, which is entitled "Additional restrictions on grant of authorisations".

Lord Butler of Brockwell: I am puzzled, like Dr Murrison. Are we to understand that you could not request communications data to establish locations of suspected persons?

Keith Bristow: If it is for the three purposes that we have set out—

Lord Butler of Brockwell: Which are—

Keith Bristow: If it was a communications website, for instance, if we wanted the internet connection record for a Twitter or Facebook account—an account that is used for communication—we could request the data, and under the Bill the data would be retained and in a format that we could access. We are talking about websites that are not about illegal content, are not communications websites—bearing in mind that these terms are

yet to be defined—and not IP resolution. Those are the areas where we understand that we could request access to the data that the service providers have retained on internet connection records.

Lord Butler of Brockwell: So we are only talking about internet connection records; we are not talking about mobile telephone records.

Keith Bristow: We are talking specifically about ICR.

Lord Butler of Brockwell: This is the distinction: we could still get mobile telephone records to establish the location of a suspect.

Keith Bristow: We could if a mobile phone was used as we currently understand it and as it has been used historically, but of course the really big challenge here is that people are communicating in a different way over the internet. We are confident in our interpretation that we could request access for communication sites, but our understanding is that we could not request the internet connection record of another type of website that might give us an investigative lead, such as one for booking travel tickets or banking.

Lord Butler of Brockwell: It seems to be a very big gap.

Q27 **Victoria Atkins**: Following on from that, would you still be able to contact let us say the travel agency, using your example, to ask whether it had business records to show that this request was made and that X number of tickets were bought?

Keith Bristow: More traditional investigative techniques could be used, but we need the lead in the first place on which travel agent we need to contact. Making the analogue-versus-digital point, the person will not have gone into somewhere on the high street; they will have interacted online. That will be the challenge.

The Chairman: It would be useful when this session is over if you gave us some written evidence with respect to some of the points that you have just made, because, as you can see, members of the Committee are interested in them.

Can I ask a question myself here? It regards current oversight powers. How do the investigatory powers that you currently possess work at the moment? What sort of oversight is there? Will there be a change as a result of this Bill?

Keith Bristow: I will ask Chris to deal with that question, but I will just make a remark to start with. We think that the authorisation and the scrutiny regime is hugely important, because public confidence is what underpins our ability to keep the public safe. It seems to us that because we cannot expose all our operational tradecraft, because we would be exposing it to the very people we want to tackle, we have to have a very clear regime that gives the public confidence that those sensitive techniques are being properly scrutinised. We think this is very important.

Chris Farrimond: There are two aspects to authorisation and oversight, and they are two quite separate parts. The authorisation process for some of our activities is internal, and some of it goes up to the Secretary of State. In each of those cases, whatever the

investigatory power is, we go through a process whereby the applicant has to write down what they require, the proportionality, the necessity, the collateral intrusion, and give their justification. Then, whatever the application is—whether it is a police Act application for intrusive surveillance, a standard surveillance application, or an application for communications data—each application contains the same different aspects of the information: the proportionality, the necessity et cetera. It will then go through the various parts of the chain. It goes to an authorising officer in every case—as I say, in some cases it goes right up to the Secretary of State. Those records are all retained and they are available for inspection at a later date.

We have two oversight regimes at present. One is provided by the Interception of Communications Commissioner's Office—IOCCO—and the other is provided by the Office of Surveillance Commissioners. The oversight regimes that they use are quite similar in that they come in for a pre-arranged inspection, on an annual basis for the most part, and we open up our records to them, give them access to our systems and let them see whatever they wish to see. For a period of a week, they will go through the records and pull out the ones that they want, and we will provide witnesses in the form of investigating officers, the applicants or whoever they wish to speak to. They will write a report based on that. Under the new legislation we envisage something that looks very similar, except that it contains one body rather than two, which we regard as fairly useful.

The Chairman: Thank you very much indeed. Moving to communications data, Miss Atkins.

Q28 **Victoria Atkins:** This is for all witnesses: how do you use communications data and for what purposes?

Richard Berry: If I might share the statistics with the Committee. Very helpfully, they were published on 20 November by the interception commissioner's office based on 100,000 communications data applications, so they are a really good data set. It varies massively. In this example, 80% of communications data applications are for the prevention and detection of crime, and 20% are submitted for interests of national security or, certainly in terms of vulnerable persons, to prevent death or injury in an emergency. So there is an 80:20 split there. From the 80% used for prevention and detection of crime, a quarter of those are in relation to police submissions for burglary, theft and robbery—volume crime.

Just under a quarter are for drug offences and just under 20% are for sexual offences. Then we have smaller and smaller chunks: 12% for harassment, 8% for homicide, fraud and deception, and violence against the person; and 1% for firearms offences. So there is a very broad spectrum of criminality.

Victoria Atkins: How valuable is this data to your investigations? I will come to prosecutions in a moment.

Richard Berry: It is essential, for example for establishing a lead, a seed upon which to build an inquiry. For example, if we take stalking and harassment, which is a very topical issue, around domestic abuse victims. To be able to establish a particular communication and an evidential line of inquiry around a victim being stalked, would be incredibly useful, in fact – vital, to support and corroborate an allegation.

Keith Bristow: We should remember that communications data for us in law enforcement is evidential. Sometimes we do not need to go any further than the communications data. We do not need to turn it into further authorisations for content. It is the "who, what, where, how".[3] Sometimes it is sufficient that we prove that to either eliminate someone from our inquiries, to find a vulnerable person or to start the process of bringing an offender to justice.

Victoria Atkins: I will ask you about context and contact in the context of prosecutions in a moment. How valuable is it in relation to successful prosecutions?

Richard Berry: That can very much depend on the case itself. In a conspiracy case where communication between conspirators is part of proving the offence, it is absolutely vital. In terms of other offences, it could be considered vital. But it could also be important, for example, if we knew a particular person was in a particular place when an offence took place. We might use CCTV evidence to corroborate and identify that person in that location. It really depends on the particular offence being prosecuted and the nature of the evidence we are able to gather.

Q29 Victoria Atkins: Drawing together not just communications data evidence that deals with context but also cell site analysis of where mobile phones are at certain times of the day, is it possible to draw a timeline of a criminal offence in action that you can then present to the jury?

Richard Berry: Absolutely. It is commonplace now to produce a sequence of events—that is the term we use—and an analytical chart on the sequence of events showing communications and where people work geolocated by their phones, and to supplement that with other forms of evidence.

Q30 Victoria Atkins: Mr Lincoln mentioned very briefly an example of a warrant not being extended in circumstances where, for example, the target perhaps has got hold of another telephone. How common is that sort of activity in organised crime gangs?

Richard Berry: Operational security is as important to criminality as it is to law enforcement.

People regularly are changing their devices, setting up false accounts and swapping devices. All those tactics and techniques are used. It takes a lot of investigation to be able to understand who is using a device at a particular time, what it is being used for at that time and how it fits into the overall picture of that criminality.

Victoria Atkins: Just to get the point into context, the length of call can in itself help prosecution counsel when suggesting to a jury, for example, that that is the moment at which the drugs were dropped.

Richard Berry: Absolutely.

---

[3] Witness correction: clarification that what should have been said is "It is the who, when, where, how." What, refers to lawful intercept which is not incorporated in the meaning of communications data.

Chris Farrimond: I offer one or two other examples. One is about the range of use of comms data. The National Crime Agency receives the bulk of referrals in respect of child sexual exploitation on behalf of the United Kingdom. Just from one source, we receive about 1,500 per month. In many cases, resolving that IP address is the only way we can identify the victim or the perpetrator. I am sad to say that in 14% of cases we cannot resolve it at all. There is no way to do it and there is no way of identifying that victim or perpetrator. That is single-source intelligence and, if we did not act on that, there is no other way of doing it. We have similar examples, as will Richard, with missing children where there is no other way of identifying them but for this methodology.

Simon York: Can I give you an HMRC perspective on this? Last year, we made just over 10,000 communications data requests. That supported 560 investigations. I think that those numbers represent the complexity and the conspiracy involved in many of these cases. Almost 100% of our requests were in relation to preventing and detecting crime in contrast to the wider needs of the NCA.

This can be in relation to anything from smuggling to tax fraud to trying to criminally exploit HMRC's repayment systems. Literally billions of pounds are at stake here. Last year, investigations where we used communications data and intercept together prevented around £2 billion loss to the UK Exchequer. That is how important it is to us.

Victoria Atkins: Is it fair to say that a lot of those investigations involve serious organised crime gangs?

Simon York: Almost all of them, yes.

Q31 Lord Butler of Brockwell: Leading on from that, was I right to understand that you were saying that internet connection records although useful are not, as defined in the Bill, sufficient to help you to identify all senders, the users of all IP addresses?

Chris Farrimond: Some IP addresses are more difficult to resolve than others. A standard home broadband is a static IP and it is relatively easy to resolve down to an address. When you use your mobile phone, your IP address is allocated to that phone just for the few seconds that you make that search and then it is allocated to someone else somewhere else in the country. It is really complicated.

The IP addresses get swapped around mobile phones, tablets and everything else around the country a lot of times per day. Trying to get complete resolution for some of the more complex ones is not possible at the moment. We believe that ICRs will allow us to close that gap quite considerably.

Lord Butler of Brockwell: Right, but it will not close it completely. I understand that you cannot always resolve IP addresses, but if you get internet connection records you can identify the users of the address.

Chris Farrimond: I am afraid that my knowledge of technology is not good enough to give 100% on this, but we believe that it will massively close the gap. It could be up to the whole amount.

Lord Butler of Brockwell: Just going back to the three purposes for which you can use it, you say that you can attribute connection from an IPR. Then you could discover that someone had been a user of Facebook. How does it help in a criminal investigation to discover that they are a user of Facebook?

Chris Farrimond: It means that we can ask Facebook. Certainly, when we are talking about vulnerable children, threats to life or anything like that, we find that communication sites of that type are extremely helpful.

Lord Butler of Brockwell: If you go to Facebook, are you going to the content and not just the communications data? Would you seek a warrant? If you did seek a warrant, would that be effective with Facebook?

Chris Farrimond: At that stage we would not need to go for an interception warrant, because we would not be intercepting communications in the course of their transmission.

Lord Butler of Brockwell: I understand.

Chris Farrimond: It would be stored data at that stage, so we would be looking for the stored data that Facebook had in that instance.

Lord Butler of Brockwell: And Facebook would be able to tell you with whom the person who was suspected had been communicating with.

Chris Farrimond: It should be able to do that, yes.

Lord Butler of Brockwell: I understand. Thank you.

Q32 Stuart C McDonald: What would you say is the operational case for 12 months in particular being the maximum time for requiring the detention of communications data and internet connection records?

Chris Farrimond: I know that the Home Office, who were here before, gave you some figures. We have a table here that it might be helpful for us to include in our written submission to you, but let me give you some examples. In a 2012 survey right across policing in the UK, of all crime types within 0 to six months approximately 84% of comms data was applicable: that is to say, when we needed it, 84% fell within the 0 to six months, 13% within the seven to 12 months, and 3% in the 12 months-plus. But that does not give the whole picture. For child abuse, only 42% fell within the 0 to six months, and 52% fell within the seven to 12 months. There are also figures for terrorism offences, sexual offences and financial offences. We can give those figures, but this quite clearly shows that the closer you are to the date, generally speaking as soon as the investigators get hold of the case they are going to want to get the data, but sometimes it takes a bit longer, for whatever reason. For instance, we do not immediately get the referrals that I spoke about a few minutes ago involving child sexual exploitation; sometimes it can take a few months for them to come through, which may be the reason for the 52%. Either way, I think it shows pretty consistently that 12 months is a reasonable point at which to draw the line.

Keith Bristow: It is worth differentiating between types of investigation. As an agency and collectively, we sometimes investigate criminals; we are proactive, so we want to know how they were transacting at that moment. With reactive investigations, of course, often we do not know what data we need until an offence has been reported to us and we are some way down the track with an investigation. I suspect that is exactly why, with child abuse, data retention is further down the line in time terms.

Simon York: The position for HMRC is a little different. Our figures show that more than 50% falls into the six to 12 month period. Indeed, quite a lot falls beyond 12 months. We are doing a lot of reactive, or historical, analysis. We have some real-time stuff, perhaps smuggling, but if it is more in the tax evasion area it can be a lot more historical; if it involves the use tax returns, we will not even do that analysis until 12 months after the year ends. We are in quite a different position from that of the National Crime Agency. Overall, we feel that 12 months is a reasonable balance to be struck, but we have a lot of cases that fall within that six to 12 month period.

Stuart C McDonald: Okay. We will obviously need to look in detail at the tables that you provide, but is there not a danger that what you are describing there is practice rather than what is essential. Is there analysis that shows that the information that you get from records that are between six and months old ends up being crucial to a case?

Richard Berry: If I may help with that, there are types of crime that require communications data perhaps two or three years after the offence has been committed and subsequently reported. Boiler-room fraud is a classic example of the picture of the criminality only emerges some years later, so clearly the 12-month period for the retention of communications data is not particularly useful for that particular criminality. Also, criminal justice processes kick in. If we are looking at an alibi or identifying further witnesses, subsequent applications for communications data up to that 12-month period can also be incredibly useful for a particular investigation because of the interests of justice and if the disclosure regime highlights that further inquiries are required by the police at that time. We have not mapped it, but I understand that that kind of data may be produced in the future and we can start to understand the value of data at a particular point in time for a particular crime type.

Q33 **Stuart C McDonald:** Thank you very much. Finally, as far as you are aware, how do such rights of access up to 12 months compare to rights of access that colleagues in other jurisdictions have?

Richard Berry: Our comparison is with the Australians, who have recently been given a two-year retention period. I understand that in the original period the data retention directive was for 24 months, so we are striking a balance in many respects. Twelve months seems to be the period when the optimal value is obtained by law enforcement.

Stuart C McDonald: In terms of internet connection records, this is fairly unique, is it not?

Richard Berry: We do not have that evidence.

Q34 **Bishop of Chester**: This is the first time I have spoken on this matter and I need to declare that I have no interests. Can I go to the question of the length of the period? Is there

frustration that it is only 12 months in serious cases in HMRC, for example, where you cannot go back beyond 12 months? Australia has fixed two years. Is this a source of frustration to you in your investigation of crime?

Keith Bristow: I think there is a need to understand the mindset of the investigator. All the best investigators are rigorously focused on doing what they need to do to keep the public safe. Chris has given numbers demonstrating 0 to six months and six to 12 months. There are also numbers that show data after 12 months that would have benefited the investigation. My sense is that there is some science that points to 12 months, but there is also the professional judgment that, when you look at the numbers, the data appears to be less relevant after 12 months. Of course our mindset that is we want every opportunity to protect the public in every set of circumstances, but that has to be balanced against other considerations.

Bishop of Chester: Are you sometimes slowed up by having to analyse seized equipment—laptops or whatever—which, as I understand it, is often in a queue, takes time and extends investigations?

Keith Bristow: Operation Notarise was an operation, led by the NCA and involving every police force in the UK, against people who were exploiting children online. We ended up seizing tens of thousands of devices that were relevant, which could be a digital camera, an iPhone: all the devices that we all understand. When you have that volume of devices, triaging those involves a lot of professional judgment about which are the most important to collect the most evidence from of the high end of high risk. We do not always get that right, because, frankly, there is not the capability, even with the private sector, to everything at pace all the time.

Bishop of Chester: Does the 12-month retention period hang over that investigation?

Keith Bristow: No, because once we have seized a media device, we have seized it. We then get to the point where we analyse its content. The 12 months is more about the data that is retained by service providers to enable us to access the data. It is not about the hard content of the device.

Bishop of Chester: So the analysis of the various devices that you have just described does not throw up the need to—

Chris Farrimond: It can do, because stored messages on a computer can point to an IP address, and, yes, we have had examples, even recently when they were one day over the date.

Keith Bristow: With victim ID, for instance, if we get an image and we want to identify the victim—a child who has been exploited—and we want to rescue that child, the reality is that we might need the communications data that sits around some of those communications to try to resolve the identity of the victim.

Q35 **Lord Strasburger:** The Counter-Terrorism and Security Bill earlier this year created the power to resolve IP addresses. How many times have you used that, and how does it differ from the power in this Bill?

Chris Farrimond: The provisions in that Act are not all in force yet. Although we use exactly the same communications service providers as our counterterrorist colleagues—so we use exactly the same access—we still cannot resolve the technology and the systems in place where the communications service provider has not yet caught up completely with the provisions of that Act. Therefore we cannot fully resolve all IP addresses, which brings me to the 14%.

Q36 **Lord Hart of Chilton**: Fifty-five years ago at university, I joined Amnesty International and I think that technically I might still be a member. That is my declaration of interest. What safeguards do you have in place to prevent unauthorised access to the communications data and other materials you hold? I imagine that the criminal mind is always at work trying to break in.

Chris Farrimond: The vast majority of communications data is held by the communications service providers. We can only access it in the certain circumstances that I have outlined around necessity, proportionality etcetera, in which case in the NCA's case, it comes into the NCA and is held on the same systems as all the other evidence we have.

It is treated in exactly the same way, to the same specification and safeguards, as all our criminal intelligence data, which is held to a high level. Although there have been various attempts to get on our website, they have only ever managed to get on the outward-facing one. They have never managed to get anywhere near the inward-facing one. That is not a challenge. We are satisfied with the security of our system.

Lord Hart of Chilton: Just to be clear, how many break-ins have there been?

Chris Farrimond: I believe there have been one or two to our outward-facing website.

Lord Hart of Chilton: And how did they come about?

Chris Farrimond: I am afraid that, again, my technical knowledge defeats me.

Keith Bristow: As regards most of the attacks that we get on our outward-facing website, the catalyst is that we have taken on some cybercriminals. The community that supports people like that do a DDoS attack on our website to try to get us to take it down. We spend considerable resource and energy making sure we keep that site secure. That is not the system where we retain our intelligence and our evidence. It is the front face and it appeals to the public that we tell them what we are doing and are as transparent as we can be. We rarely take it down, but sometimes as the result of a DDoS attack we have had to do so to protect it.

Lord Hart of Chilton: How much has that cost you?

Keith Bristow: I would need to come back to you with a number, but it is significant.

Simon York: Similarly from an HMRC perspective, we hold this information on secure systems in secure buildings and we have specially selected and trained staff who are the only people with access to this type of material.

Lord Hart of Chilton: And you have not had any breaches?

Simon York: No.

Richard Berry: The single point of contact in David Anderson's report. they have pin numbers and they are all vetted to a high standard and they work in secure environments. There are a range of security measures, as well as the physical security, to ensure that there are no breaches of unlawful access of that information.

Lord Hart of Chilton: So, as far as you are concerned, there have been no breaches?

Richard Berry: Absolutely.

Lord Butler of Brockwell: The Inland Revenue had a notorious example of where they lost CDs in the post. Are you absolutely sure you have systems that prevent anything like that happening with this sort of data?

Simon York: Absolutely. After that event, which was quite some years ago now, there was a very comprehensive review of all our security processes. Interestingly, the data that was allegedly on those discs has never surfaced in any way to be used in criminality or otherwise in the UK.

Lord Hart of Chilton: Did you ever recover it?

Simon York: No.

Keith Bristow: From an NCA perspective, we invest huge amounts of energy and time in data security. What I could not do is give you a 100% cast-iron guarantee that there will never be a breach. When you mix well-intentioned people into any of these systems, it needs only one failing for data to get into the public domain. But within what is physically and legally possible, we treat this information security as our top risk.

Q37 **Matt Warman**: Can you talk me through what value equipment interference provides your organisation and what justification there is for you to be able to conduct equipment interference?

Chris Farrimond: We use property interference at the moment, which is authorised under the Police Act. We use it for a range of purposes, ranging from pretty much every-day relatively routine activities right up to far more high end. The difficulty is that trying to describe any of those techniques in this setting probably would be inappropriate, but I would certainly be very happy to explain them in a great deal more detail if we had the opportunity to do so.

Matt Warman: More generally, in that case, how often do anticipate being required to use equipment interference in the future?

Chris Farrimond: That is quite difficult to answer, because I could not have predicted the IP revolution that there has been or the digital change that we have seen. The change from traditional telephony into IP-based communications has been enormous and the pace has been really difficult to keep up with. I could not make any prediction about just how much we would use this. I suspect that our limitation would be around our own resources and

our own capability rather than the demand. The demand for quite a lot of the services that I am allowed to manage within the NCA outstrips supply.

Keith Bristow: To give you a trend, I think it is fair to say that as law-abiding citizens it is no different—more of what we do now is online using digital devices. I imagine that the trend will peak, but I think that we will be doing more rather than less that reflects the behaviour of the criminals who we are targeting.

Richard Berry: To give a police perspective on this, we use equipment interference regularly, really for tracing vulnerable and suicidal missing persons.

The other point I would like to make is that there has to be some consideration from our perspective of the integrity of the information contained on a device that is interfered with. For example, to comply with the requirements of Section 69 of the Police and Criminal Evidence Act on the integrity of computer information, there might be considerations perhaps prohibiting the creation of data purporting to be communications data on that particular device or perhaps removing such data from that device. The evidential integrity of that device might be particularly important. Perhaps we can expand on that in a written submission.

Q38 **Matt Warman:** Finally, on demand versus supply, do your organisations currently have the capabilities technically and in terms of manpower to do what is needed? Do you anticipate seriously being able to ramp that up?

Chris Farrimond: We have the capability, and I anticipate that, if required, we could ramp it up, yes.

Keith Bristow: The change for the NCA and the transformation programme that it is going to go through—the Government announced the funding for that last year—mostly relates to our digital capabilities. As criminals go online, we need to be as adept in the digital environment as we are in the physical environment. Those capabilities are going to be invested in on behalf of the whole law enforcement community and not just us, because we provide those to our colleagues in HMRC, for instance.

Richard Berry: RUSI recommendation 5 as being that law enforcement should have a comprehensive digital investigations intelligence programme. A number of colleagues are here and we are part of that programme. Building capabilities is certainly one of those priorities.

The Chairman: Thank you very much indeed. Again, apologies for the delay because of the votes. This has been a fascinating session and we look forward to receiving your written evidence to supplement what you have told us today.

Keith Bristow: Chairman, do you mind if I just reiterate Chris's offer? We want to be open and transparent with the Committee and the public viewing this or reading the report are hugely important. However, we cannot betray all our tradecraft to criminals.

The Chairman: Of course not.

Keith Bristow: There is an open offer to the Committee, and I know that I speak for my colleagues as well; if you want to look at what we do, whether in a comms data unit or about equipment interference, we will brief you at a higher level of classification to help with your deliberations. Thank you for your time.

The Chairman: That is very generous of you. Thank you very much indeed.

Robin Simcox, Henry Jackson Society (QQ 216-223)

Evidence heard in public Questions 216-223

Oral Evidence

Taken before the Joint Committee

on Monday 21 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Suella Fernandes MP, David Hanson MP, Shabana Mahmood MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Lord Hart of Chilton, and Lord Strasburger.

Witness: **Robin Simcox**, Henry Jackson Society, gave evidence.

Q216 **The Chairman:** A very warm welcome to you both. Thank you so much for coming along this close to Christmas. We very much look forward to hearing your views on this extremely important Bill that Parliament is now considering. Apologies, too, for running a little late. I hope that it has not disturbed you. I will ask the first question, which will give you an opportunity to give the Committee your initial thoughts on the Bill. Do you think that it strikes the right balance between privacy and security? If it does not, how could it be improved? Should any other powers be included? It is really a very general question about your views on the Bill.

Robin Simcox: Many thanks for the invitation to speak here today. It does broadly strike the right balance. I might be in a minority of some of the people you have heard from so far in that I did not think that RIPA was an entirely unworkable disaster, but I appreciate that some clarity was needed with regard to bulk collection, which the Bill provides. It is also very useful for putting the powers in one place, one piece of legislation. The one thing that I might add as a word of caution is that the balance is right as the Bill is currently drafted, but I would be somewhat concerned if, during fierce negotiations in Parliament, it got watered down significantly on things such as bulk collection and the internet connection records. Those are quite fundamental powers needed by law enforcement and the intelligence agencies. The Bill is a successful piece of legislation that strikes the right balance at present, but I add that caution about losing any further powers contained in it.

Professor Christopher Forsyth: Lord Chairman, I am not an expert in surveillance, interception or security, so in a way my view on these matters is simply that of an ordinary citizen rather than an expert. I am afraid that, given the times we live in, it is inevitable that greater weight will be given to security over privacy in the balancing process than might otherwise have been the case, or even tolerable, in more placid times. To that extent, I recognise that the Bill provides for significant inroads on privacy, but it seems to me as an ordinary citizen, not an expert, that those inroads are justified.

The Chairman: Thank you both. That is very clear and concise.

Q217 Lord Hart of Chilton: We have heard in our evidence sessions a great deal about three interrelated subjects. I have three questions that I will put together. What is your view of the proposed double lock for authorisation of certain warrants? What is your understanding of judicial review principles? What is the correct balance between the respective roles of Ministers and judicial commissioners in the authorisation of warrants? Before you answer, I put to you an answer that Shami Chakrabarti gave at an evidence session here on 9 December. She said, "A double lock would mean, 'I can substitute my decision on the merits for yours'. Traditional judicial review means, 'I look at the way you made your decision, but I do not substitute my own for yours'. You have to be procedurally irregular or to have made a completely insane decision that no Secretary of State could make". I just wonder, since I know that you have written a paper on the question of judges taking the law unto themselves, what you think. First, is it a true double lock? Then, what do you understand the judicial review principles to mean?

Professor Christopher Forsyth: I will start with the judicial review principles, which used to be quite straightforward but are much less so now than they were. In 1984, in the GCHQ case, Lord Diplock said that there were three grounds of judicial review: procedural irregularity; illegality; and irrationality. The picture that he presents of judicial review is a situation in which you identify any one of those three grounds. If any one of those grounds is identified then the decision is open to be quashed. Outside those areas, where no ground has been established, the decision-maker—in our context, the Minister deciding whether to authorise a warrant—would be free to decide as they judged best in particular circumstances. There was a considerable degree of decision-makers' autonomy.

In his famous dictum where he set all this out, Lord Diplock also looked forward to a time in which proportionality might become part of the grounds for judicial review. So it has proved, whether it comes about through common law or through the effect of the Human Rights Act, that proportionality has assumed centre stage. This has had the disadvantage—some people would say the advantage—of making the process much more uncertain than it would otherwise have been. No one can be against proportionality in one sense—after all, we are all against taking a sledgehammer to crack a nut—but it is very easy to describe proportionality at the level of a slogan of a more abstract having the means and ends in balance. It is very easy to have that sort of description, but in reality it means a great deal of uncertainty. It is a very bold person who can predict the outcome of the decision-making process once proportionality enters the field. The principles of judicial review have become a much less certain concept than they would have been 30 years ago.

There is another consideration here that suggest that judicial review principles are, in a way, unsuitable or would have to be thought about a bit more carefully. I mentioned the three grounds of procedural irregularity, irrationality and illegality. Procedural irregularity is, of course, the principle that people should be heard and given the opportunity to make their case before a decision adverse to their interests is taken. That, of course, cannot happen in the kind of context that we are talking about—the interception of communications. It means that a whole slice of judicial review principles has been discarded for the purposes of this exercise. The effect of that would primarily be that the judges or judicial commissioners would tend to look more intensively to scrutinise more anxiously the decision-making process to make up for the fact that one is not hearing what

the person adversely affected—whose communications will be intercepted—thinks about this. Is that enough food for thought?

Lord Butler of Brockwell: Can I just ask a supplementary? Would the Bill be better without Clause 19(2), about applying "the same principles as would be applied by a court on an application for judicial review"?

Professor Christopher Forsyth: That depends on what you want to achieve by the Bill.

Lord Butler of Brockwell: Would it give more effective judicial control if that clause was removed?

Professor Christopher Forsyth: I suspect that if one was to strike out that clause you would end up with more effective judicial control. In fact, there would be a real danger of judicial duplication of what the Secretary of State decides.

Lord Strasburger: Would you call that a double lock?

Professor Christopher Forsyth: One might very well call it a double lock.

Lord Hart of Chilton: So on that basis the judge would be able to supplant the Home Secretary's decision with his own?

Professor Christopher Forsyth: I suspect that would be the outcome if you were to excise the subsection on judicial review. In my view that would be a retrograde step, although it would be open to Parliament to do it if it wished to. The Secretary of State ought to be making decisions on grounds different from those of the judicial commissioner. The judicial commissioner should make up his mind and assess the legality of the process, whereas the Secretary of State must surely show that she has acted lawfully but will take many other considerations into account. For example, if you were to intercept the communications of a foreign dignitary or diplomat there might be all kinds of consequences to that decision that it is right for the Secretary of State to take into account, but it seems to me inappropriate for a judge to take into account. But if that is what you want—the same criteria being applied to both elements of that decision-making process by the judge and Secretary of State—then so be it, but what are you achieving by the double lock if they are essentially deciding the same grounds?

Q218 Suella Fernandes: I should declare an interest that I was a student of Professor Forsyth's many years ago—you probably do not remember; I was a face in a crowd. Where do you think the line should be drawn between judicial and executive decision-making power in the context of warrantry?

Professor Christopher Forsyth: As far as common or garden serious crime is concerned, it has long been the case that these decisions—to issue a search warrant, for example—are taken by a purely judicial and not an administrative process. That is absolutely right. It does not seem necessary to me to have the Secretary of State's involvement in warrantry extending to the investigation of serious or organised crime. But when one is talking about national security or economic well-being, it is appropriate that the Secretary of State should take these wider considerations into account, which are inappropriate for the judge to take

into account. That is where I would draw the line. Of course, in all these areas, half-covered by secrecy or sometimes fully covered by secrecy, it is very difficult to lay down a principled position, but that would be my position. I am sorry that I do not remember you attending my lectures. I hope you benefited from them.

Suella Fernandes: I did, yes. Would you say that judges should not be involved in the issuing of warrants when it comes to national security matters?

Professor Christopher Forsyth: The Bill as it stands is a reasonable compromise in that judges can go into necessity and proportionality but they are to do so according to the principles of judicial review. If they do so according to the principles of judicial review—which means in this context that they will intervene only if they discover some ground for judicial review or a legal flaw in the decision—that seems right.

Q219 **Dr Andrew Murrison:** Professor Forsyth, how would you distinguish national security from serious crime? You appear to be suggesting that we should treat the two separately for the purposes of the powers discussed in the Bill. My second question is: should we not seek some sort of confluence with the rest of the Five Eyes community in the way that we determine warrantry and the various other powers in the Bill?

Professor Christopher Forsyth: Clearly, there will be cases where national security and serious crime overlap; for example, an organised money-laundering scam raising money for use in terrorist attacks or something of that kind. This is a definitional problem. Once national security became involved, I would think that it would trump ordinary serious crime and you would apply the national security criteria. But I recognise that that is a question of definition. On your question about seeking some sort of congruence with the Five Eyes community, that is so far beyond my understanding and experience—I know that the Five Eyes exist; I know very little more about them. It is clearly in the public interest that there should be close co-ordination among the Five Eyes. Whether that is achieved is above my pay grade.

Dr Andrew Murrison: I wonder if the Henry Jackson Society has a view, given its provenance.

Robin Simcox: Speaking for myself, close co-operation between the Five Eyes in this area is important but if you look at the issues to do with extraterritorial jurisdiction, what we need goes beyond the Five Eyes. If it was possible, there would be some kind of international treaty governing some of these areas because some of the things that DRIPA and the draft IP Bill look to do—for example, serving warrants against CSPs, making requests for data that are lawful in the UK but may contravene American law if those CSPs are based in the US—is where we are constantly running into the problem of overlapping jurisdictions and if there can be some progress made, as distant and unrealistic as that currently seems, considering some of the other countries that are involved in this, on an international treaty governing these things, that has to be something that we look at, to go beyond even the Five Eyes.

Q220 **Matt Warman:** We heard in the previous session about bulk interception being one of the most controversial issues. This always comes back to whether an operational case has been made for this sort of invasion of privacy. In your opening answers, you both indicated

that you thought that it had. Can you elaborate a little more on the operational case that you see has been made?

Robin Simcox: I think it has; it has to me, certainly. One thing that the UK Government have tended to do, as opposed to the US Government, who have sometimes not been as completely savvy on this as they could have been, is provide some of the real-life case studies of where this has been useful. The Government did this even in the draft Communications Data Bill back in 2012. David Anderson provided some examples and in the guide to the IP Bill further examples are provided. This is not just about terrorism; it is about fraud, other serious crime, stopping child exploitation, drug trafficking, et cetera. Providing those real-life examples resonates; it is too abstract without them. But I would also take it beyond that and say that the debate should be less about capacity and more about the strength of the oversight. It has been put to me in the past that, for example, we are relaxed about the Army having sophisticated weaponry because we trust the culture; we trust the oversight and that it will not be used against the population. You can apply a similar paradigm to our interception capacities. Having world-class intelligence-gathering is not a bad thing; it needs to be accompanied by extremely strong and responsible oversight.

Professor Christopher Forsyth: I agree. From my reading of the Bill and the associated documents, the case seems to be made for the necessity of bulk warrants to be granted in appropriate circumstances and the safeguards built into the Bill seem pretty considerable to me.

Q221 **Lord Butler of Brockwell:** Do you think that the draft Bill provides sufficient protection for legal privilege? It was put to us last week that there could be an absolute protection for legal privilege on the grounds that if a lawyer was involved in misdoing, that would remove legal privilege by itself because it would be a form of inequity. If you had a crooked lawyer, you could have legal privilege enshrined in the Bill but that would not stop the authorities intruding upon them.

Professor Christopher Forsyth: It is true that if the lawyer is found guilty of misconduct, he would not be able to rely on privilege. The difficulty is that the lawyer may be guilty of misconduct but you may not be able to prove it; you only suspect it. Again, I think the Bill has got it about right. I have no difficulty with that.

Lord Butler of Brockwell: Thank you. Did you want to add to that?

Robin Simcox: On the legal privilege side of things, I welcome the role of the judicial commissioner on this because there have been examples of the misuse of RIPA in the past, Andrew Mitchell and Plebgate being a very prominent example. But we cannot rely just on the role of the judicial commissioner here. There have to be properly trained single points of contact. Again, it goes back to the culture of the institution—the TS Eliot line about "dreaming up systems so perfect that no one needs to be good". There also needs to be a culture where powers are not wilfully and clearly misused, as seems to be the case on an isolated number of occasions with regard to RIPA and journalistic sources. So I welcome the role of the judicial commissioner but there needs to be a change in the culture as well, it seems.

Lord Butler of Brockwell: Yes, so with the role of the judicial commissioner, you think there is sufficient protection both for legal privilege and for journalists. Am I right in interpreting you both in that respect? Okay, thank you.

What about MPs? The protection there is the Secretary of State, the judicial commissioner and the Prime Minister. Is that sufficient protection for Members of Parliament, bearing in mind that the Prime Minister may be of an opposite political persuasion from the MP in question?

Professor Christopher Forsyth: The crucial safeguard there is the judicial commissioner. I do not think that giving statutory form to the Wilson doctrine would change very much, because it is difficult to see how that statute would ever be justiciable, other than perhaps providing a clearer audit trail when one of these decisions is made. One quite understands that individual MPs of one party might not believe that the Prime Minister is much of a safeguard when he belongs to a directly opposed party, but that is what the judicial commissioner is there to do: to see that there is no skulduggery in the approval of the warrant. If the judicial commissioner refuses, it is not going to get to the Prime Minister.

Lord Butler of Brockwell: Mr Simcox?

Robin Simcox: I have nothing further to add to that.

Lord Butler of Brockwell: Would there not be some advantage in putting the Wilson doctrine in law in the sense that if it is known that in due course at the appropriate time it has to be reported to Parliament that a Member of Parliament has been intercepted, this would make the Secretary of State more wary of doing it in unnecessary cases?

Professor Christopher Forsyth: I agree. That is what I mean by there being an audit trail, but I just do not see Clause 22 actually being litigated under in the judicial review court, so it would have no legal effect.

Q222 Suella Fernandes: I have a follow-up question on the issue that Professor Forsyth raised about judges and Ministers. There has been talk in our evidence sessions about the accountability and transparency of Ministers versus judges. Lord Carlile, who was the independent reviewer of terrorism legislation, has cautioned against the involvement of judges because of the lack of transparency, electability or accountability compared with Ministers. Could you comment on the comparison between the two arms and the importance of that in this context?

Professor Christopher Forsyth: I would echo what Lord Carlile says there. I recognise that there is a very strong political drive towards having the judiciary involved in this process, but the judiciary are not accountable in the way the Executive and Ministers are. Forgive me for putting it quite as starkly as this, but one would hate to see, after there had been some sort of dreadful outrage and the death of innocents, the Home Secretary facing an angry House of Commons and saying, "Well, I authorised a warrant to intercept these communications to find out what these wrongdoers were up to, but the judge refused it", bringing judges into the maelstrom of a political dispute. That it is putting it starkly, but that is the point about accountability: that given the nature of these powers, there needs

to be proper accountability, and the Executive and Ministers are accountable in a way in which judges are not.

Suella Fernandes: In what way? Could you elaborate?

Professor Christopher Forsyth: Ministers are accountable in that they will come before the House of Commons and Committees of this kind and have to justify themselves and answer difficult questions. The judges are not going to do that.

Suella Fernandes: I want to move on to another issue, overseas examples, and ask both of you whether there are any other countries that we could look to for guidance that have grappled with this issue.

Robin Simcox: This partially goes back to your previous question, too. The involvement of some democracies where the system and role of the judiciary are comparable to that of the UK—Australia, Canada, France and Germany—is significantly less than that of the UK. So there is that overseas example. The example of New Zealand, where the inspector-general of intelligence and security need not be a former judge, is sometimes cited, but I do not think you need to look to New Zealand to see how that can work well. Someone just mentioned Lord Carlile and David Anderson, neither of whom were sitting judges but both of whom were excellent lawyers who did a terrific job in the independent reviewer chair. Both have publicly done a great job in explaining that role to the public. They go on the radio and television and explain the role, and are an excellent link between the legislation and the general public's understanding of it. In this area we may decide that it needs to be a sitting judge, but the Carlile and Anderson examples provide a useful model for us here.

Dr Andrew Murrison: How do you feel that the idea of ministerial accountability in the areas we are discussing today can be lifted from the purely theoretical, since invariably when Ministers are asked about security matters in the Commons they will reply that it is not custom and practice for Ministers to comment on security matters?

Professor Christopher Forsyth: I do not think they are quite as reticent as that when they come before a Committee in private such as the intelligence services Committee. Is that not where their accountability comes through?

Dr Andrew Murrison: It is not very transparent, and I wonder whether you think that there are ways in which their decision-making can be made more transparent in real time. Of course, accountability can come to pass many years down the track, but that is of little help in the here and now.

Professor Christopher Forsyth: I think it is inherent within the intelligence services that things have to be kept secret that in an ideal world would not be kept secret, so I have difficulty in seeing how there would be accountability in real time. One can imagine that after a particular outrage and disruption and the death of civilian innocents the Home Secretary would come to the House and explain what was being done to track down the wrongdoers and to do whatever could be done to assist the victims, but would be extremely reluctant to provide any clear operational information about operations that might still be ongoing.

Lord Strasburger: But it is illegal for a Minister to discuss a warrant in public.

Professor Christopher Forsyth: I am not sure that that is the case.

Lord Butler of Brockwell: It is the case.

Dr Andrew Murrison: Do you think there may be grounds for reviewing that, given the double lock, which of course is different from practice in other countries with which we can reasonably be compared?

Professor Christopher Forsyth: Yes. I am surprised by that, quite frankly, but I think there would be occasions on which you would expect the Minister to be able to deal with the individual case, and that might allow them to discuss the warrant. So, yes, I think that should be changed.

The Chairman: Last but by no means least, Baroness Browning.

Q223 **Baroness Browning:** Thank you. I think Mr Simcox answered in reply to Ms Fernandes what I was going to ask, but I just wonder, Professor Forsyth, whether we could hear your views on the issue of the office of the Investigatory Powers Commissioner being led by a commissioner who has held a senior judicial position—at least as high as a High Court judge? What is your view of alternative models, such as the one used in New Zealand? I know that we have heard about other examples, but would you let us have your views?

Professor Christopher Forsyth: As I said earlier, I am cautious about the use of judges in this area. I recognise that there is a political need and a political demand for judicial involvement, but because of that general approach I see nothing wrong in principle with your inspector-general being a non-judge, as in New Zealand. If you look at some of the things that the New Zealand inspector-general has been doing, she has been acting in an entirely proper way in holding the services to account but in a way in which a judge might act. I think there are potential advantages to not having a judge, who inevitably is tied by the detail of the evidence, moving slowly and so forth. These are aspects of the judicial character. It may be good to have a non-judge dealing with these situations.

I would agree, too, that we have such good examples here of both Lord Carlile and David Anderson QC—non-judges carrying out these different legal tasks and doing so, if I may say so, with considerable success and very impressively. So I do not think that the inspector-general need necessarily be a judge, but it seems to me that very often the decision to involve the judges has been taken essentially for reasons of trust, because the other branches of government are not trusted sufficiently, whereas judges are trusted. I am not sure that that is entirely correct. When one looks at these things, as far as one can tell, not being privy to any secret information, these matters are dealt with very conscientiously and according to law entirely within the Executive at the moment.

The Chairman: Thank you both very much indeed. It has been a fascinating session. We wish you both a very happy Christmas.

Home Office (QQ 1-25)

Evidence heard in public Questions 1-25

Oral Evidence

Taken before the Joint Committee

on Monday 30 November 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Bishop of Chester, Lord Hart of Chilton, and Lord Strasburger.

Witnesses: **Paul Lincoln**, Director, National Security, and **Richard Alcock**, Director, Communications Capability Development Programme, OSCT, Home Office, gave evidence.

Q1 The Chairman: I apologise for the fact that we are two minutes late. Welcome to our witnesses. We have, of course, seen Mr Lincoln in another capacity. We have until between now and about 5.30 pm. As is normal with these arrangements, all members of the Committee will ask questions. I will kick off in a second, but I remind Members of the House of Lords that they should declare any interests when they ask the question. Perhaps I could ask the three of you a very general question to begin with. Could you give a few brief remarks on what the draft Bill proposes and why it is necessary?

Paul Lincoln: The draft Bill responds to the three reports that were commissioned in this area: the recommendations from the Independent Reviewer of Terrorism Legislation, David Anderson QC; the review that was done by the Royal United Services Institute at the behest of the then Deputy Prime Minister; and the report by the Intelligence and Security Committee of Parliament. All three reviews agreed that the powers associated with communications and the data associated with communications should be brought together in one place to make them more clear and transparent. This draft Bill attempts to do three things. First, it brings together, as requested, the powers already available to law enforcement in this area. It makes them clearer and more understandable than they have been in the past. Secondly, the draft Bill overhauls the oversight arrangements. In particular, you will have noticed that we have proposed a double-lock authorisation for the most intrusive powers, which consists of a Secretary of State authorisation as well as a judicial commissioner authorisation. Thirdly, the Bill ensures that the powers are fit for the digital age, so restoring capabilities that law enforcement would previously have had in relation to communications data by bringing in powers for internet connection records.

The Chairman: Thank you very much. I do not know whether your colleagues wish to make any additional points. If not, arising from that and to make it clear to the Committee, which of the proposed powers are brand new, and which of them are being rewritten in new legislation?

Paul Lincoln: This Bill is very much about transparency and oversight, which the three reviews all said needed to be improved, as this is about powers. The Bill brings the existing powers together. The only new capability that is provided for relates to internet connection records.

The Chairman: Yes, but what does that mean for oversight?

Paul Lincoln: It not only brings the double-lock system that I talked about for the most intrusive powers, involving Secretary of State and judicial commissioner authorisation, but it establishes a new Investigatory Powers Commissioner, bringing together the existing three commissioner bodies and providing additional resources and additional technical and legal expertise.

The Chairman: Thank you very much. Other than the expiry at the end of 2016 of the provisions of DRIPA, what would the impact be if we did not have this Bill?

Paul Lincoln: If we did not have this Bill, we would lose a once-in-a-generation opportunity to provide some of the additional oversight mechanisms that I talked about a moment ago. In terms of the powers and capabilities, a new capability is provided for that in effect restores powers that used to exist around internet connection records. We have provided data as part of the associated documentation with the Bill, which sets out the operational case for that.

Q2 **The Chairman**: Just one more question from me before I hand over to my colleagues. What has been the impact of the Digital Rights Ireland case and the Court of Appeal decision in the Davis case on the powers and the wording of the Bill before the Committee?

Paul Lincoln: The Government responded to the Digital Rights Ireland case by passing some fast-track legislation in 2014, the Data Retention and Investigatory Powers Act, which took account of the ruling on Digital Rights Ireland. However, on the back of that, a judicial review was brought against those powers, which Parliament had voted for. That judicial review, in the Divisional Court, found two reasons for which the powers were incompatible with European legislation. Since then, a Court of Appeal ruling has said provisionally that it did not think that Digital Rights Ireland set out a minimum set of standards for Governments to comply with, and on the back of that the Court of Appeal has remitted this to the court in the European Union. Therefore, we have considered that position and the powers and the associated processes for which Parliament voted in 2014.

Q3 **Lord Strasburger:** Could you tell us in which Acts there would still be surveillance, data acquisition or equipment interference powers after the passage of this Bill?

Paul Lincoln: We have taken the opportunity to bring those into this, when it comes to the primary purposes relating to accessing communications data or content, but the Police Act, for example, would still allow equipment interference for other purposes.

Lord Strasburger: Are those the only ones?

Paul Lincoln: Those would be a good example. Similarly, the Intelligence Services Act would allow that for the intelligence agencies.

Lord Strasburger: Will you be able to give us a list in writing?

Paul Lincoln: We can write to the Committee.

Lord Strasburger: Secondly, you indicated that all the powers except one already exist. I think that we need a bit more clarity on that, particularly about whether all the existing powers have been recently authorised by Parliament. Given that CNE was not avowed by the Government until February 2015, bulk interception was first mentioned in the ISC report in March 2015, and the collection of bulk communications data was not avowed until the Home Secretary did so this month, it would have been impossible for any of those, as well as several other powers in the Bill, to have been specifically debated and authorised by Parliament. Do you agree that it is high time that many of those existing powers were debated by this Committee and by Parliament?

Paul Lincoln: The powers exist already. As David Anderson said, this Bill is an opportunity to bring that more clearly into focus and to allow Parliament, as we take this forward, to take an explicit view on all the powers in the Bill.

Lord Strasburger: I think you missed my point, which was that the three powers that I mentioned and others have never been specifically debated in Parliament. Do you not think that it is time that Parliament did debate them?

Paul Lincoln: Parliament now has the opportunity to debate these powers as this Bill is passed.

Q4 Suella Fernandes: What is it about the character and scale of the threat that makes this legislation necessary?

Paul Lincoln: If people look at the products in the public domain, the Joint Terrorism Analysis Centre has independently set the level of threat to this country at severe, which means that an attack is highly likely. You have also heard that the Home Secretary, the Prime Minister and the intelligence agencies have said that seven plots against this country have been disrupted this year that otherwise would have ended up probably in some form of fatality. Equally, figures published worldwide indicate 12,000 terrorist attacks in 91 countries in 2013, the last year for which figures were publicly available.

Q5 Shabana Mahmood: How confident are you that the powers in the draft Bill are effectively future-proofed?

Paul Lincoln: By bringing the powers together we have looked at the question of future-proofing. The critical thing is internet connection records and restoring capabilities that law enforcement have traditionally had as part of that. Richard no doubt will talk later about some of the processes that we have been through in talking to communication service providers and other technology companies about the specifics of the technology.

The Chairman: Let us move now to Mr Hanson, who I know has a number of questions.

Q6 Mr David Hanson: As regards the old system versus the new system of judicial authorisation, I am interested in whether there is any likelihood of additional time pressures on decision-making.

Paul Lincoln: Each authorisation is currently considered on a case-by-case basis, and that takes a certain amount of time. There is no set time for looking at the authorisation. It

needs to be done on the merits and the complexity of the case. Additional time may be needed for physically having two people involved in that decision-making process. The system that was put in as part of the draft Bill allows for urgency procedures. If there is a time-critical situation, a judicial commissioner can sign off under that procedure up to five days afterwards.

Mr David Hanson: Could we expect that, for example, in the Christmas period, the new year period or Easter period? Is that feasible and doable? In an urgent circumstance, would that be acceptable?

Paul Lincoln: In urgent circumstances, we have systems now in place where we deal with Secretaries of State. We have rota systems in place and we can access Secretaries of State out of hours to work through those systems.

Mr David Hanson: In the event that the judicial commissioner disagrees with a recommendation from a Secretary of State, what is the mechanism for that to be examined? Is that it?

Paul Lincoln: If that happened, the judicial commissioner would have to set out in writing the reasons for that refusal. The Secretary of State can have a discussion with that judicial commissioner to work through the issues. For example, it might be that collateral intrusion into a particular subject was too great when looking at necessity and proportionality. That is the kind of discussion that we have now.

If you got to a position where, having gone through that process, the judicial commissioner still disagreed, the Secretary of State can ask the investigatory powers commissioner to look at this. If the investigatory powers commissioner disagrees, that is as far as that will go and the warrant will not come into force if they disagree.

Mr David Hanson: What of that discourse would at any time eventually be public in the event of accountability for one or both of those officials being held by the House of Commons or the House of Lords?

Paul Lincoln: If something went wrong, as we have seen in the past, inquiries are often held. The Intelligence and Security Committee led an inquiry into the circumstances surrounding the murder of Fusilier Lee Rigby, for example, which took into account the way in which these things work. Similarly, the commissioners hold to account an oversight of the process that is put in place.

Mr David Hanson: One final question. How many of these do you estimate would be deemed to be urgent, given what happened historically? What is your assessment of the number that will be urgent?

Paul Lincoln: In reality, we think that this will be very few percentage points of the overall number of cases. We have not provided a specific estimate, but it will be a very small number of cases—probably the majority would be where there is an imminent threat to life.

The Chairman: What about the definition of urgency? Is it self-defining or will we have some sort of guideline? I am sure that there will be grey areas.

Paul Lincoln: We have not set out in the Bill a definition of urgent. In reality, a warrant will be considered urgent only if there is a very limited window of opportunity to act. We would expect to set out guidance in a code of practice, as is usually the way in which these things are set out.

Lord Butler of Brockwell: If a warrant has been issued—

The Chairman: I do beg your pardon. We have to adjourn for five or 10 minutes while Members of the House of Lords vote.

The Committee suspended for a Division in the House of Lords.

The Chairman: We were in the middle of a sentence.

Lord Butler of Brockwell: If a warrant is issued for one purpose, can the information that it provides be used for another purpose? For example, if a warrant is taken out for someone suspected of terrorism and it throws up evidence of offences under Customs and Excise, could the information be used without taking out another warrant?

Paul Lincoln: Certain purposes are set out for the intelligence agencies where they are allowed to share information along the lines of their statutory purposes. If I take your example the other way around, if you discover in a tax evasion case that someone was involved in terrorism, the practice would be that you would take out a separate warrant to do with the terrorism and run the necessity and proportionality test for that.

Lord Butler of Brockwell: Thank you. But the information that was first obtained under the tax evasion warrant could then be used to justify a further warrant for terrorism but a further warrant would be needed.

Paul Lincoln: A further warrant would be the practice to be followed through. Yes.

Q7 **Dr Andrew Murrison**: I am worried about the five days, because the Five Eyes community does not put up an artificial distinction between urgent and routine, since all warrants have to be certified by a member of the judiciary rather than a politician. I wonder why we have lighted upon five days. Are we seriously saying that we may not be able to get a judge to pass a view within five days? I would find that extraordinary. Perhaps we might consider whether a lesser period of time was appropriate for matters that are deemed to be urgent.

Paul Lincoln: Among the various recommendations from the reports, the Royal United Services Institute report, for example, recommended a period of 14 days for an urgency procedure, which we considered too long. We alighted on a period of five days as a maximum that would allow for sufficient time when the system may be running at its hottest if there was a particular set of counterterrorism investigations going on. In reality, we would expect decisions to be made much more swiftly than that.

Lord Strasburger: We know that the Home Secretary signs on average six of these warrants a day. Could you tell us approximately how much time she spends on it?

Paul Lincoln: I cannot give you the precise time that she spends on each warrant. She has said to the House of Commons that she spends more time on warrantry than she does on any other topic.

The Chairman: Thank you very much. We now move on to Baroness Browning, who has a number of questions that she would like to ask.

Q8 Baroness Browning: Thank you. I have to remind the Committee of my interest in the register as chair of the Advisory Committee on Business Appointments, which gives advice to senior members of the security and intelligence community when they leave office. Could I ask you about the request filter system, which I think is new? Could you explain to us how the request filter system works for applications to access communications data? In explaining how that works, perhaps you might like to give us an idea as to the correlation between the new system and fishing expeditions and whether there is a vulnerability there.

Richard Alcock: The request filter is fundamentally a safeguard, the purpose of which is to limit the amount of data that goes through to law enforcement. People access comms data right now through a system of robust oversight, with the appropriate checks and balances and with necessity and proportionality at its heart. The request filter cannot be used unless a particular case has been made that it is both necessary and proportionate. By way of example of how the request filter might be used, a criminal may have committed three crimes in three locations at three different times. A request for comms data may go in about who was at a particular location in those three instances. Without the request filter and subject, obviously, to the approval being granted for that kind of request, the full array of data would be made available to law enforcement. The request filter would filter out all the irrelevant data and just identify the individuals or entities that were in those three locations at that particular point in time, so it would reduce the amount of irrelevant information that would go through to law enforcement. It does not allow for fishing, just to address that point, because you can only make a request when that is necessary and proportionate for a specific instance, which is obviously judged by investigating officers and with the appropriate oversight.

Baroness Browning: You do not think there is any fishing risk at all in the system.

Richard Alcock: No, because the same tests apply to the existing comms data approval regime.

Paul Lincoln: It may be worth adding that the Bill provides for a new offence around the abuse of powers around communications data; it provides a criminal offence for people who abuse the powers as part of this.

Baroness Browning: The Joint Committee on the Draft Communications Data Bill, as you are probably aware, identified a risk to the request filter system. Why do you think there is a difference of opinion? What has changed to minimise that risk?

Richard Alcock: The Joint Committee concluded that it was a safeguard while acknowledging that there was a risk. The risk has been mitigated by virtue of the criminal

sanction that may be imposed with inappropriate access to the information that could be accessed through the system.

Baroness Browning: Sorry, did you say "criminal sanction"?

Richard Alcock: The new offence, which Paul just outlined, of inappropriate access to comms data mitigates that risk.

Paul Lincoln: There is oversight by the Investigatory Powers Commissioner as a starting point in terms of all the powers in the Bill, but in addition to that we have greater defence in the Bill to make sure that in extremis if you are wilfully trying to abuse the system, a criminal sanction is available. There are also administrative and other sanctions available to the Government.

Q9 Lord Hart of Chilton: This is a question about judicial review principles. We know that the judge or judicial commissioner, when looking at the warrant, must apply the same principles as would be applied by a court on an application for judicial review. We have seen that there are some who say that that is not a great power because it is interested in process rather than the merits. I would like you to help the Committee by explaining what you understand to be the judicial review principles for the purposes of the Bill.

Paul Lincoln: As we said before, the Bill allows for a double-lock process. The judicial commissioner comes second in that process. The principle of judicial review is well established. Lord Pannick in particular set out that he thought that the test that was set for this Bill was the right one. In examining the data that is put in front of them as part of the request, they will see exactly the same information as the Secretary of State has and they will be able to determine whether or not the decision was lawful and rational. In doing so, they will also be able to determine whether or not the particular action was both necessary and proportionate. The necessary and proportionate test is, of course, exactly the same one that the Secretary of State is looking at.

Lord Hart of Chilton: We have seen David Pannick's article from 12 November, but we are interested in finding out the extent to which a judge could use what is called the Wednesbury principle in deciding whether or not no reasonable Secretary of State could come to the conclusion that a warrant was justified. Does the Wednesbury principle apply in this case, as that is a judicial review principle?

Paul Lincoln: The specifics here are that two things will be critical: first, that they decide in the first place that the action is rational and lawful; and, secondly, that it is necessary and proportionate. Those are exactly the same tests as the ones the Secretary of State will be looking at.

Lord Hart of Chilton: But how far could the judge go in deciding that the Secretary of State had stepped outside the remit?

Paul Lincoln: If a judge thinks that the Secretary of State has stepped outside the remit, it is for them to decide so and to say that they do not think that the warrant should come into force. Then there is the process that we described earlier about whether we appeal after that.

Lord Butler of Brockwell: What is the difference, if any, between "rational" and "reasonable"?

Paul Lincoln: I will have to ask one of my legal colleagues and write to the Committee on that one.

Lord Butler of Brockwell: It is an important point, because, as Lord Hart said, the question is whether the Wednesbury test—that no reasonable Minister could have taken the decision—should be applied. If I may say so, I do not think that you answered that. You used the word "rational", but what we really want to know is whether the Wednesbury principle applies.

Paul Lincoln: Okay. We will come back on the specifics of the principle.

Q10 **Dr Andrew Murrison**: On the subject of targeted interception warrants, if I had applied for and had been granted such a warrant but I wanted to change it in some way, how would I go about doing it?

Paul Lincoln: A process is set out as part of the draft Bill stating how modifications can be made to a targeted interception warrant.

Dr Andrew Murrison: Presumably those would be of a minor nature, or would they be fundamental?

Paul Lincoln: As for making a change to a warrant, if I was a criminal or a terrorist, let us say, and a decision had already been made by a Secretary of State and a judicial commissioner to put my communications under interception, then the decision had been made that it was both necessary and proportionate to intercept Paul Lincoln's communications in that manner. The example in that situation might be that I decide that I am going to buy a new mobile phone and, in doing so, I now have a new telephone number. Rather than necessarily going back and testing again that I am somebody who needs to have my communications intercepted, a senior official could make the change to say that that new telephone number could be added to that warrant.

Dr Andrew Murrison: At what point would you need to have the involvement of, first, the Secretary of State and, secondly, a judicial person?

Paul Lincoln: If you were to have situation where you then said—I do not know—a new person was coming along and a new circumstance, you would ask for a new interception warrant.

Dr Andrew Murrison: Through the whole process, so both the Minister and the judge?

Paul Lincoln: For both the Minister and the judge.

Dr Andrew Murrison: How does that differ from the situation that applies to equipment interference warrants?

Lewis Neal: It definitely needs some of the approach to modifications. Equipment interference follows the approach that we have taken to the original decision. In the case of SIA it will go through the departments of state, the Foreign Secretary and the judicial commissioner, whereas for law enforcement it will go straight to the judicial commissioner.

Dr Andrew Murrison: So why the difference?

Paul Lincoln: The approach follows the style point in how the authorising is done. In a case involving the intelligence agencies, for example, there is already someone separate from the chain of investigation who is looking at authorising that. In the case of the police, you are looking at doing this to add that additional safeguard as part of that process.

Dr Andrew Murrison: Presumably, there is also someone in the police looking at this too.

Paul Lincoln: Yes. Sorry.

Dr Andrew Murrison: You suggested that the difference was because in the intelligence agencies there is a specific person dealing with this.

Paul Lincoln: But you then have a separate department of state, which is independent from the body that is looking at it, which also considers that separately, whereas in the police you have that organisation itself looking at it rather than saying that there is a department of state, for example, separately looking at the authorisation. It is an additional safeguard.

Dr Andrew Murrison: Otherwise you just have the one.

Paul Lincoln: Otherwise you just have the one.

Dr Andrew Murrison: Do you think that is sufficient? It sounds a little odd to me.

Paul Lincoln: It effectively provides a form of a double-lock in terms of those modifications.

Dr Andrew Murrison: Why, then, should the handling of the equipment interference warrants and the targeted interception warrants be so different?

Paul Lincoln: That reflects effectively the starting point in saying who should be required to authorise that, and it follows consistently the starting point from—

Dr Andrew Murrison: It just seems to me that it unnecessarily complicates it.

Paul Lincoln: Our intention was to keep it simple.

Dr Andrew Murrison: Obviously it did not work. It has confused me. I admit that I am only a simple soul, but it seems to have established the two on different levels with different procedures. I wonder whether the matter might be simplified by simply having the same process without distinguishing it.

Paul Lincoln: That may be a judgment the Committee comes to.

Dr Andrew Murrison: Would it be a major issue in terms of workload?

Paul Lincoln: We would obviously look at what the implications might be in detail.

Q11 Lord Strasburger: Why does the phrase “judicial review” in respect of warrants appear in the draft Bill?

Paul Lincoln: We have talked about that by saying that those are the principles under which a judicial commissioner would look at the authorisation of—

Lord Strasburger: I am just trying to understand why the judge would not look on the same basis as the Home Secretary.

Paul Lincoln: As I said, the consideration they will give follows the point about whether it is rational and lawful, and whether it is necessary and proportionate, which is the same test as the one the Home Secretary or the Foreign Secretary applies.

Lord Strasburger: So most judicial reviews are rather redundant, are they not?

Paul Lincoln: I think we said that we would write back on the specific principle. As I said, we are quoting both the report from RUSI, which said that this was an appropriate way to approach this, and some of the recommendations made by David Anderson. In this space, this seems to be the appropriate approach to take.

Q12 **Suella Fernandes**: Before the judge reviews a decision, how will the evidence before that judge compare to the evidence before the Minister?

Paul Lincoln: The judicial commissioner will have the same information as the Secretary of State.

Suella Fernandes: How does the test applied by the judge compare to that applied by the Minister?

Paul Lincoln: They will look at the rationality and lawfulness, and will consider the necessity as part of that decision.

Stuart C McDonald: Will the judicial commissioner be able to question members of the intelligence services, for example, when considering warrants?

Paul Lincoln: You would expect there to be potential for some conversation to go on. At the moment, conversations would happen with the agencies to try to clarify potentially the methods that people are using. If someone was trying to conduct surveillance or an intrusive activity against a particular suspect, you may question whether collateral intrusion was appropriate. Those are the kinds of conversations that happen now. You would expect similar conversations in the future.

The Chairman: To clarify that, when authorising a warrant, clearly the judicial commissioner and the Secretary of State need not be together physically. They could be in different buildings and different places, but would it be at more or less at the same time?

Paul Lincoln: When looking at the warrant itself?

The Chairman: Yes.

Paul Lincoln: Not necessarily. For more routine warrants, it may be a period of days before a judicial commissioner can do it.

The Chairman: Would that be the five days that we talked about?

Paul Lincoln: It could be a number of days.

Lord Hart of Chilton: Unlike the judicial review normally, there would be no third party representations, would there?

Paul Lincoln: The investigatory powers commissioners could look at the system and decide whether they think this is something on which they need further representation. We have not put a system in a place where we are expecting people to be making additional submissions on top of those provided. We have said that we will provide training to those who will become judicial commissioners, and we are working with the Lord Chief Justice's office to set out what that might be.

The Chairman: Who would look at the warrant first?

Paul Lincoln: The process is that the final person who has the say is the judicial commissioner. It will have gone through a Secretary of State first.

The Chairman: The Secretary of State and then the judicial commissioner.

Q13 **Shabana Mahmood**: I just want to look at the issue in relation to privilege. Obviously, Clause 16 relates to Members of Parliament and the additional safeguards that will apply to communications between a constituent and an MP. I was interested in the rationale for giving those additional safeguards for Members of Parliament but not for legally privileged communications between a client and a lawyer or the protection of journalistic sources. What is the reason for the differential treatment of all three things, which are quite important to our constitutional arrangements?

Paul Lincoln: The Bill provides now for all forms of interception. The requirement of a judicial commissioner to sign off is the key difference from the situation today. All forms of interception now require the involvement of a judicial commissioner. That is a significant step that people would appreciate. The difference with Members of Parliament is that it also requires consultation with the Prime Minister, which reflects the wishes of certainly Members of the House of Commons. There was a debate about that some weeks ago on the Wilson doctrine, which went to the Investigatory Powers Tribunal. This is the result of those debates.

Q14 **Shabana Mahmood**: Moving on to communications data, which is about context rather than content, as a lay person I would expect content to be the most valuable bit of what you might be looking for, but the context has also been described as gold dust. It is very important. How would you describe the relative value of context as opposed to content when it comes to communications data?

Paul Lincoln: Both forms are very important but in their own different ways. For example, communications data is used in 95%[4] of all criminal prosecutions. It is an essential tool for law enforcement in particular to identify, for example, missing persons or to rule people

[4] Witness correction: the figure refers to 95% of serious and organised crime cases, handled by the Crown Prosecution Service

out of an investigation and try to minimise more intrusive techniques to gain content from that. It is very valuable in its own right.

Shabana Mahmood: So the oversight regime is less stringent than it would be for content. Given that you are both saying that they are both valuable, why is there different treatment when it comes to oversight?

Paul Lincoln: Oversight is by the Investigatory Powers Commissioner in all senses and all the powers in the Bill. There is perhaps a question about the authorisation, which you talked about, where Parliament has traditionally said that communications data is a less intrusive form than content, and the authorisation regime that maintains a very similar process that we have today reflects that.

Shabana Mahmood: Do you agree that it is a less intrusive form?

Paul Lincoln: Personally I do, and the Government have reflected that in the way in which the Bill has been put together.

Shabana Mahmood: Is that view shared across your sector, as it were?

Paul Lincoln: Yes. Law enforcement and the intelligence agencies will say that that is the same.

Q15 **Shabana Mahmood**: What is the rationale for Schedule 4? I can understand why police forces and intelligence agencies need to have access to communications data or are entitled to see acquisition of the data. I was slightly nonplussed by local authorities being on that list, given that by 2020 it would be a big deal if they can trim a tree or fill a pothole, rather than acquiring communications data, which might be beyond their resources.

Paul Lincoln: A wide range of bodies have access to communications data. The Financial Conduct Authority might use it for conducting investigations into insider trading. The Maritime and Coastguard Agency might use it for finding missing people at sea. For local authorities, ways in which to investigate might include rogue traders, environmental offences or benefit fraud.

David Anderson said that if you have relevant criminal investigation powers you should have the tools associated with that, and communications data is one of them.

Lord Hart of Chilton: Just one point. I did not quite get the answer to the question about the justification for allowing legally privileged communications to be intercepted. As you probably know, the Bar Council has raised strong objections to the fact that privileged communications between an individual and a lawyer are not safeguarded. Why is that?

Paul Lincoln: Special considerations apply to legally privileged material. Their safeguards are set out in codes of practice as part of this. Unfortunately, there may be situations in which people try to abuse the privileges available to them. Therefore, there is not a complete bar on such activity in terms of interception.[5]

[5] Home Office clarification: The policy intent is to make clear that special considerations apply to legally privileged material. The additional safeguards that apply to this and other particularly confidential information are set out in codes of practice. This is because the privilege attached to the contents of communications

Lord Hart of Chilton: Some might not consider that to be sufficiently justifying it, but that is the answer. Thank you.

Q16 Lord Butler of Brockwell: I understood that the Home Secretary said in her statement that local authorities would no longer have access to communications data, and I cannot find them in Schedule 4. Could local authorities in certain circumstances select this data?

Paul Lincoln: There are two points there. Local authorities have to go to a magistrate before they are able to access communications data. That was introduced in, I think, 2012. There have been some instances where potentially the powers have been abused. Part of the rectification of that was to bring in a magistrate.

The second question is probably to do with internet connection records, where the Home Secretary is on record as saying that local authorities will not be allowed access to internet connection records for any purpose.

Q17 Lord Strasburger: Are you aware that most experts consider communications data, especially that including internet connection records, to be at least as revealing as content these days? A former NSA general counsel said that it absolutely told you everything about someone's life and that if you have enough metadata you do not need content. A former director of the CIA said, "We kill people on the basis of metadata". Do not the most intrusive elements in communications data need a higher level of authorisation than the current entirely internal process?

Paul Lincoln: We agree that parts of communications data are more intrusive than others. As part of that, the Bill sets out the different authorisation levels, which are internal authorisation levels, with those that are more intrusive having to be signed off by a higher person in terms of the rank structure in any given organisation recognising the sensitivities behind it.

Q18 Dr Andrew Murrison: Can I just press you a bit on communications data and the long list of authorities that have access to this. I think you are referring in 2012 to the case that Poole Borough Council lost at tribunal, where it was found to have overstepped the mark.

Do you feel it is sufficient for these authorities to apply simply to a magistrate to gain the access that they say they require, or do you think that list needs to be revised? I certainly know which I think.

Paul Lincoln: Our approach has been to continue the process which requires a magistrate to sign off, which is an additional level to what it would be in other organisations. On top of that they have to go through a mandated single point of contact for quality assurance before going to make the request. The National Anti-Fraud Network is part of that, which has been pretty successful, and David Anderson recommends the NAFN as one of the most successful bodies in this area.

---

between lawyer and client is important and must be protected. However, it is in the nature of the intercepting agencies' work that they will sometimes legitimately need to intercept communications between people and their lawyers in the interests of preventing or investigating serious crime or terrorist activity.

Dr Andrew Murrison: Do you feel that their access to this data will mean that their skills in other means of detecting fraud might become degraded? Do you agree that fraud covers a whole load of things from the most serious crime to the frankly trivial?

Paul Lincoln: To put the numbers into perspective, only 0.5% of requests made for communications data overall are made by local authorities. It is a relatively low number in comparison with investigations in the round.

Dr Andrew Murrison: That is no justification though, is it?

Paul Lincoln: For access in their own right?

Dr Andrew Murrison: Not ensuring the job that we have to do to scrutinise this legislation at this stage would not be justification for us to overlook this particular thing; simply to say that it is so small that it does not really matter?

Paul Lincoln: I was not suggesting that. But in terms of the safeguards put behind this, certainly the Government have responded to that previously, and we have kept the same method, which involves the magistrate and the single point of contact through the National Anti-Fraud Network.

The Chairman: Can we move now to Miss Fernandes? Is your voice holding up?

Q19 **Suella Fernandes**: I think it is getting worse. Why has 12 months has been chosen as the timeframe for data retention?

Paul Lincoln: You could choose a range of different periods for which you might have retention. The data retention directive previously allowed for a timeframe between six months and 24 months. The UK decided to adopt a maximum of 12 months when it first introduced its legislation in this area. The 12 months was considered to be the right balance as to the level of intrusiveness in holding that amount of data. It was done on the basis of surveys by looking into the way in which law enforcement used the powers.

The critical reason for going up to 12 months is child sexual exploitation cases. Certainly when a survey was done on this in 2012, 49% of all requests made in child sexual exploitation cases were for data between 10 and 12 months old. That is a very significant period, which is reflected in the position that we have taken.

Suella Fernandes: What assessment has the Home Office made of 18 months?

Paul Lincoln: You could go further than that, but this is the position that we have taken historically. Other nations have gone further. The Australians are a good example. They recently passed legislation to go for 24 months' worth of data retention, but we thought that 12 months struck the right kind of balance between those two things.

Suella Fernandes: In terms of communications service providers and their holding of data for 12 months, has there been any assessment of the cost and workability of that?

Richard Alcock: As you would expect, we have had a number of meetings with the communications service providers on which we would likely serve notice under the new

legislation. The retention period in the Bill obviously reflects the retention period proposed in this legislation. We have a very good relationship with the CSPs on which we serve notices now. We have worked with them throughout the summer, and before then, to think about the likely data volumes and to work out the estimated costs for the retention of internet connection records specifically. Those are contained within the impact assessment.

It is important to note that it is an estimate. Why is it an estimate? That is because CSPs systems change all the time. There are mergers, acquisitions and so on, but it is the best estimate right now based on the work that we have been doing with them over the past few months.

Paul Lincoln: It is also worth clarifying that the period for a maximum of 12 months for communications data is already current practice in terms of data being stored by those that are under a data retention notice. So that is not a new proposal.

The Chairman: You said earlier that one of the reasons for the 12 months was the investigation into child abuse, but you also implied by that that other investigations might not need the retention for 12 months. Could there be a sliding scale of holding this material according to the nature of the investigation?

Paul Lincoln: There is a question, therefore, between retention and access. To be in a position where you can access data in relation to child sexual exploitation, you have to retain all data associated with communications for up to 12 months to able to make those connections. The question of access is then perhaps complicated in terms of practicality. You may end up missing a significant proportion of investigations. If I was to say that a firearms investigation needed data that was six months old, I might make a connection to a child sexual exploitation case that also needed nine to 10-months-old data, or to a prostitution ring that needed something else, and I would not necessarily be able to make the links between those different investigations by having access for different times.

Mr David Hanson: Can I just be clear? You said that the costs in the impact assessment are to cover the costs of the 12-month period. Are the Government entirely covering costs to service providers and any expanded retentions?

Richard Alcock: The costs are to cover reasonable costs for the additional retention of the internet connection records, so there is provision in the—

Mr David Hanson: So how much is the impact assessment figure? From memory, around £240 million is related to that cost.

Richard Alcock: It is £174 million over a 10-year period in relation to internet connection records. Right now, under existing legislation, in the last financial year we spent around £19 million on data retention, so broadly speaking we are doubling the cost of data retention.

Mr David Hanson: So, again, does the assessment over the 10-year period include an assessment of the expansion of the market, of different types of material, of different types of activity, of the capacity overall of organisations, of new providers entering the market? How do you arrive at that figure?

Richard Alcock: We have worked with industry over summer to look at the likely data volumes and the costs associated with that volumetric growth over time, so even though I gave the example of £17 million a year, the reality is that the cost may go up over that time. But, as I say, we have been working very closely with the comms service providers on which we are likely to serve notice to underpin the facts and figures within the impact assessment.

Mr David Hanson: So when we have the service providers in front of us in the near future and we ask them the same question, will they tell us that they are content with the amount of resource that they give them, or not?

Richard Alcock: As I say, we continue to work with the comms service providers to look at the estimates of volumetric growth and how we would go about implementing those systems over time. We make balanced judgments on the service providers on which we serve notices, and we sometimes have to make hard choices about where we put data retention notices. But, again, as I say, it is all about working very closely with law enforcement, to identify where most value can be accrued from retention, and with comms service providers to understand—

Mr David Hanson: One final question from me. Is that therefore a budget that you have to spend, or is that an assessment of the costs?

Richard Alcock: It is currently an estimate of the likely cost for implementing internet connection records over a 10-year period.

Mr David Hanson: With certain providers.

Richard Alcock: Yes.

Lord Butler of Brockwell: Why does the taxpayer have to meet the cost at all of these records being retained? Why can it not simply be a condition of providers providing services that they retain these records at their expense?

Paul Lincoln: What we have tried to do, and as we have done in the past, is to make sure that companies are not materially disadvantaged by having to meet the requirements of government in this space.

Stuart C McDonald: Just a quick follow-up question first of all. I was interested in what you said about doing surveys of police work in relation to retained data. You commented on the 49% of all requests in child sexual exploitation cases being for data between 10 and 12 months old. In how many cases where the data was between 10 and 12 months old did that data prove to be essential to the outcome of the case?

Paul Lincoln: You are probably better asking the law-enforcement colleagues who are giving evidence after us, but communications data is often the only start point for child sexual exploitation investigations.

Stuart C McDonald: Thank you very much. Also in relation to data retention, obviously one of people's key concerns is security. When you are retaining data on such a huge scale, how can you be sure that that data is going to be securely retained?

Richard Alcock: Our retention systems are built to meet stringent security requirements, working in partnership with comms service providers to ensure that they meet very rigorous standards. Those systems are overseen by the Information Commissioner. We have annual accreditation. We have, typically, dedicated stores in which the comms data is held, which can be accessed only by law enforcement through encrypted data links and so on. As I say, it is a high priority for us to ensure that security and integrity. We have a very good track record of maintaining the security of existing data retention systems, and we are looking very much to build on that good practice, working in partnership with the comms service providers.

Stuart C McDonald: A related concern is about the definition of service provider. Someone suggested that the way that is defined just now means that pretty much any form of software provider could end up being saddled with these obligations to retain records over 12 months old. Do you have a response to that concern?

Richard Alcock: We will not be putting notices on every service provider as you suggest; we make balanced judgments about which organisations we would serve retention notices. Obviously I cannot go into detail about the organisations that we would intend to serve notices on, but we have been working with every organisation that would be likely to have a notice served on it.

Paul Lincoln: It is also worth saying that there is a route of appeal for those organisations if they think that this is a disproportionate thing to do. They can appeal to the Secretary of State, and there is a process involving a technical advisory board, which will consider the technical implications and cross-implications as part of that.

Q20 **Stuart C McDonald**: My final related question is about whether or not it is going to place UK-based communications service providers at a competitive disadvantage, in that some non-UK citizens will simply choose not to trade with UK-based providers.

Paul Lincoln: Part of that question is similar to Lord Butler's question. In that respect, that is one of the reasons why we give reasonable costs back to the companies as part of that. Was there something else behind your question?

Stuart C McDonald: Not just in a financial sense but in the sense of the different obligations that are going to be placed on UK-based providers and non-UK-based providers. Some might simply say, "If there is going to be all this storage of my data, I'm just not going to use a UK-based provider".

Paul Lincoln: The powers in this are not new; they have been known about for some time. Data retention is a widespread power that is used in many different countries, so I would think that that set of differentiators is likely to be limited.

Q21 **Lord Butler of Brockwell**: Going on to one or two technical issues, we understand that because IP addresses are not unique, you cannot identify a sender solely through the IP

address, but you can identify them through the internet communications records: in other words, through what they have been to. So is it correct that providers keep records of internet connections?

Richard Alcock: Some do not at the moment. The purpose of the legislation is to ensure that they can where served under notice. The whole operation of communications over the internet is very complex. If you will indulge me, if you have a smartphone, that phone will then communicate with your comms service provider and you will have an IP address and what is known as a port address between those two nodes. There will then be another IP address and another port address between your comms service provider and the destination, whatever web service it is. So you have constantly changing IP addresses and port numbers, and because of that sometimes having the destination IP address or the internet connection record address is the only way of identifying a person to a communication.

Lord Butler of Brockwell: So have you reached agreement with the providers on how this is going to work technically? Do you have a clear agreement with them about what you are going to serve notices on for retention?

Richard Alcock: We have ongoing discussions with a number of comms service providers, as I mentioned before. Those service-provider systems are constantly changing. We have a good relationship with the service providers on which we are likely to serve notice, and we have a good understanding of their current technical systems. During all the conversations that we have with them, at no point have they said that it is impossible to implement.

Lord Butler of Brockwell: So when we see them, will we hear from them that they think that the exercise of these powers is practicable?

Richard Alcock: I hope they will say it is possible. They will say it is hard. They will say that there is more work to be done, because their systems are constantly changing. But, as I say, we have been having a productive dialogue with them for a number of months, specifically about internet connection records.

Q22 Lord Strasburger: Before I ask my question, I should mention that the Home Office estimate for the cost of implementing the communications data programme, which in terms of storage was considerably smaller, was, from recollection, £1.8 billion over 10 years.

I want to talk about security. There are many breaches of cybersecurity every week. Examples from the last few months include: TalkTalk; giffgaff; a 13 year-old boy hacking into the email account of the current director of the CIA and accessing sensitive government data; and the theft of 4 million personnel records of US government employees, probably by the Chinese. How can the public have any confidence that their personal data, stored by the Government at their ISPs, will not be stolen, and who will be responsible when it is?

Richard Alcock: The retention systems are built to stringent standards, and those standards are set by the Home Office. Systems do not go live unless they have been independently tested and accredited. We are very confident in the arrangements that we have to maintain security of the data retention systems, and I cannot say more than that. We completely

understand the threat, and because of that we put a lot of effort into ensuring that integrity.

Lord Strasburger: Who advises on that?

Paul Lincoln: We do not want to sound complacent, but the Information Commission provides independent oversight of those arrangements. As I say, it is one of four principal things that we look at: the physical security of buildings, infrastructure and the rest of it; technical systems, including firewalls and the like; personnel vetting systems, where that might be appropriate; and procedure—the processes, training and the like, which are put behind that.

Richard Alcock: And all that is accredited on an annual basis.

Q23 **Matt Warman:** I would like to talk a bit about encryption. We all know that, on the one hand, encryption is absolutely essential for everyday life. On the other hand it has also meant that some bits of communication that you were able to access are now not visible. There is provision in the Bill for the Secretary of State to make regulations to impose obligations on telecommunications service providers "relating to the removal of electronic protection applied by a relevant operator to any communications or data". Does that mean that there is provision here to remove encryption, and, if so, how?

Paul Lincoln: I should start by saying that the Government are a strong supporter of encryption for information audit purposes and information assurance purposes. Some £860 million was spent on the national cybersecurity programme, and of course the spending review last week announced another £1.9 billion for looking at this. GCHQ probably does more for this country's cybersecurity than any organisation.

The Bill itself in effect replicates the existing legislation, which has been in place since 2000, and says in effect that we should be in a similar position to that of the real, physical world, where, as David Anderson says in his report and others have said, you do not want there to be places where people are allowed to go unpoliced and ungoverned. The same should apply in the internet world. So when you have taken the steps with regard to necessity and proportionality, you can place a requirement on companies to provide you with content in the clear.

Matt Warman: I understand that you might wish that to be the case, but in practice everything from my message from an iPhone to another iPhone is now encrypted end to end. Does this provision propose to tackle something like that, and, if so, how?

Paul Lincoln: Not everything is encrypted end to end. It would not suit the business models of many companies to encrypt their information end to end, and many of those companies would not tell you that their systems were unsafe, which they are not. But you have to think whether or not in the right circumstances you will ask people to unencrypt information, and people do do that for us.

Matt Warman: Where companies currently think it is right to provide a commercial service that involves end-to-end encryption, are you trying to tackle that, and, if so, how?

Paul Lincoln: All we have done is replicate exactly the same service. If you are providing a service to UK customers and the Secretary of State and a judicial commissioner think there is necessity and proportionality in order to be able to provide that information, those companies should be required to provide that information in the clear.

Matt Warman: Do you think that is practicable?

Paul Lincoln: We are not setting out for anyone how they should do that. It is for others to say what the best way is for them to achieve that. The Government do not want to hold the keys to encryption or anything like that. That debate happened a long time ago. The Government decided that they did not want to do that and have not set out technical standards in this regard. They are saying, "In the right circumstances, we want you to be able to provide this information in the clear".

Q24 **Matt Warman:** I will come on to bulk equipment interference in that case. Could you all outline what bulk equipment interference is as far as you are concerned, and when it might be proportionate?

Lewis Neal: There is a difference between targeted equipment interference and bulk equipment interference. For targeted equipment interference, you might know the identity of the individual or the piece of equipment you are targeting. For bulk equipment interference, which is targeted at activity overseas and where the intelligence picture and the levels of information about your target are less, you would be able to seek authorisation to target equipment where you did not necessarily know a particular device or the individual that you were targeting.

Matt Warman: And when might that be a proportionate response?

Lewis Neal: Where you have a specific intelligence requirement overseas and you do not have the information but you might have an idea of the locality of the risk or the threat, the necessity would be set out and you would consider the proportionality of that action and potentially the types of information that you were seeking to obtain. Typically in that situation you might look at equipment data that enabled you to further identify the target and to develop a case for activities that have a higher level of intrusion.

Matt Warman: So you would see equipment interference in lay terms as happening at the level of internet infrastructure, rather than—

The Chairman: Order, order. There is a Division in the House of Lords. We will be back in 10 minutes.

The Committee suspended for a Division in the House of Lords.

The Chairman: Again, apologies for democracy. Perhaps I may move now to Miss Atkins who I know has a number of questions.

Q25 **Victoria Atkins:** How does the data collected as a result of equipment interference differ from interception material?

Lewis Neal: Equipment interference is a range of techniques to acquire communication information from a variety of bits of equipment, from computers to mobile phones, whereas interception is making communications available while they are in transit. In practice you could use both tools to obtain the same levels of information, be it equipment data, communications data or content, but that would depend on your objective and exactly how you were using the tools.

The legislation will require the agencies and the Secretary of State to consider the most proportionate way to acquire the data. If equipment interference may enable you to collect a certain bit of data, essentially you would use that technique as opposed to using interception where you may be collecting more data and a higher level of intrusion when it is not proportionate.

Victoria Atkins: Intercept material is not admissible, or indeed disclosable, in court legal proceedings. Why is it deemed acceptable for material acquired through equipment interference to be eligible for use in legal proceedings but not material acquired through interception?

Paul Lincoln: In principle the Government have no objection to having interception used in evidence. It is the default that you would want to have material used in evidence, but there have been a number of reviews into this over the years. The last was in December 2014, which concluded that it was not possible to introduce an intercept-as-evidence regime in this country. The benefits would not outweigh the risks and the costs associated with doing so. There have been seven or eight reports on this, which have all come to that same conclusion.

Victoria Atkins: I know that colleagues might be wondering why intercept materials is admissible in other countries under different regimes. Is it fair to say that those countries have different disclosure regimes that perhaps are not as demanding of law enforcement and prosecution agencies as the disclosure regime in this country?

Paul Lincoln: There is a combination of questions about disclosure. In particular, if you were to intercept someone's communications and were trying to use that in court, you would potentially need to intercept every bit of communication that they have done and transcribe all that so that you could set out whether or not there was information that was contrary to that that would be used to bring a prosecution. There are other ways in which other countries' regimes differ. We are not the only country in the world: for example, the Irish do not have an intercept-as-evidence regime either.

The Chairman: Thank you very much indeed. I am sorry that it has been a bit disjointed, but it has been an extremely valuable and interesting session. Many thanks for your time.

Lord Strasburger: Chair, may I correct my statement? I should have declared an interest. I have been a member of Liberty since I was a young man.

The Chairman: Thank you very much indeed.

James Blessing, Chair, Internet Service Providers Association (IPSA) (QQ 116-126)

Evidence heard in public Questions 116-126

Oral Evidence

Taken before the Joint Committee

on Wednesday 9 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Lord Henley, Lord Strasburger.

Witness: **James Blessing**, ISPA Chair and CTO of Keycom, gave evidence.

Q116 The Chairman: Welcome and thank you for coming along to give evidence to us on a Bill which is extremely important for the country and for organisations and companies like yours. I am going to ask you a fairly straightforward question to begin with, but if in answering it you want to make a general statement, please feel free to do so. How extensively has the Home Office engaged with you with respect to the provisions contained in the Bill?

Adrian Kennard: Not at all really. As a small ISP, the only involvement we have had is that ISPA—the Internet Service Providers Association—was invited to a briefing after the Bill was published to try to explain it to us. That is the only involvement we have had.

James Blessing: As ISPA we tried to engage beforehand. We made representations. There was not a long dialogue until after the Bill was presented. It has been a bit difficult on that side of things. As a service provider—I do both—there has been no conversation whatsoever.

The Chairman: It is perhaps important to explain to the Committee that Mr Blessing acts in two capacities, with his own company but also as chair of ISPA.

Q117 Lord Butler of Brockwell: In the absence of discussions with the Home Office, to the extent that you have been able to think about what is proposed by way of separating communications data from content, have you any view about whether it is practicable?

James Blessing: It is practicable as in it can be done. It is not practicable in many senses because it is not clear what is required to be done. Because the Bill does not on the face of it say exactly what is required to happen—what information is required to be captured, what format it is to be stored in and how it is to be made available—it is very difficult to design a solution that works and does all the things it needs to do, which is secure, safe and retains the data needed by law enforcement to continue its investigations. Part of the issue is that the Internet connection records do not exist. They are not a thing. They are not generated in normal business. We do not have them. They are a new thing that has been

created, and because they are not defined it is difficult to say how you would go about creating them.

Adrian Kennard: I have concerns about the definitions as well. The communications data depend hugely on the context of the communication. The definitions make something like a phone number communications data, but that should only make sense in the context of a telephone call. If it is buried inside an email, is it still communications data? It seems that the Bill could consider it that, and could give the Home Secretary power to have a snoop on the content of information to pull out anything that is an identifier, like an email address, a phone number or someone arranging a meeting. It is quite important that the definitions relate to the context of the individual communication.

Lord Butler of Brockwell: Where do you expect that definition to be made? Are you expecting it to be made in the code of practice—clearly there will be further work—and how long do you think it will take?

James Blessing: In an ideal world we would like it in the Bill itself. Having what is required clear and transparent in the Bill makes it easy for everyone to understand what is being collected. The Internet industry is slightly different from many other industries in the fact that we depend on each other to be able to do what we do. Therefore, we tend to discuss in open forums solutions to problems that we commonly have. If collecting Internet connection records became a thing and it was clearly defined—"This is what they are"—it would be something we would sit down in rooms and discuss and for which we could come up with solutions that worked for us. Our networks are all very different. They are all designed, grow organically over time, and change and adapt depending on the types of customers we have, so there is no single solution that will work for everybody. Even with two networks that look very similar, their solutions will not work, because they will have some exceptions that cause a problem. Unless that is clearly codified in the Bill itself, it makes trying to work out what is going to happen very difficult. The code of practice has not been published. Even a draft version of the code of practice has not been published, which again leads to the problem that there has been no scrutiny, no review of it. From my understanding, the Internet connection records are going to be defined in individual orders from the Home Secretary, which leads to another problem in that we cannot discuss them with each other. There may be operational reasons—we do not know—but the problem is that we have no visibility and no way of talking about them because we are prevented from discussing them with any other party.

Adrian Kennard: It is worth pointing out that the previous regulations provided a very specific, clear menu on the face of the regulation as to what could be retained—telephone numbers for telephone calls, text messages and email addresses. It would be massively helpful if the Bill spelt out exactly what data need to be recorded; what there is currently an operational justification for retaining should be spelt out in the Bill. That would help massively with these discussions, because we would be able to understand what we might be asked to record.

Lord Butler of Brockwell: Would it not be a little inflexible to put it in the Bill, because as technology changes and the world goes on, you would need amendments? Would it be

sensible for it to be in a statutory instrument so that it is there in public and everybody can see it?

James Blessing: It would, as long as it is some form of document that is published so that we can all see it and discuss it. Statutory instruments would work as well, as long as they can be discussed in public.

Adrian Kennard: If that is to be the case, it is important that what the initial SI will be is available when the Bill is considered by Parliament, because what data needs to be recorded has a massive impact on costs. I know technology changes over time, but I am not sure that granting the Secretary of State such wide powers with those very vague terms is justified simply in the name of future-proofing. It does not usually work.

Lord Butler of Brockwell: Directions from the Home Secretary are unsatisfactory because they are confidential. Is that the point you are making?

Adrian Kennard: That is important.

James Blessing: It is important.

Q118 **Dr Andrew Murrison:** I do not have much more to ask on this particular bit, Chairman, except to say that the definitions are rather refined in this piece of legislation compared with its predecessor legislations, which in part this is meant to replace. I am getting from you that we have a long way to go yet for this to be in any way a workable document, and that you would prefer to see the codes of practice or statutory instruments published at pretty much the same time as the Bill, since without those the Bill is pretty pointless, is it not?

James Blessing: Yes.

Dr Andrew Murrison: Is that it, in a nutshell?

Adrian Kennard: Yes, I think so. You say they are more refined. The previous regulations were very clear—telephone numbers, email addresses. This is about identifiers that could refer to equipment somewhere in very vague terms.

Dr Andrew Murrison: Forgive me, I was thinking more about electronic data than about telecommunications—telephone—data, which I accept are much easier to record and are recordable in any event for billing purposes. This is in a different space entirely, is it not?

Adrian Kennard: Yes. I am sure ISPA and telecommunications operators would be happy to work on coming up with some clear definitions to help you, to specify in clear terms what an Internet protocol address is and what an email address is, to give you an idea of what those data are and how they could be written down.

Dr Andrew Murrison: I am slightly disappointed that the Home Office has not already done so, because we are presented with this whopping great draft Bill, yet we are pretty unclear about the definitions; indeed, when questioning your predecessors on the panel and asking them to put it on a Likert scale of zero to 10, where zero is rubbish and 10 is extremely good, they said it was zero, which is a cause for concern.

Adrian Kennard: That sounds a bit negative.

James Blessing: There are some nice bits in the Bill that clarify a few things in a nice way. They are a rare beast within the Bill as a whole.

Adrian Kennard: I get the impression that the Home Office has spoken to the larger ISPs. It said as much in the meeting we had. In order to come up with the cost estimates it must have a clear idea what information it is asking for. While we would love to help specify the data that can be collected so that that can be put in the Bill, the Home Office has just left it out. I do not think it is that it does not know. It must have an idea to get the costing.

Dr Andrew Murrison: It is simply relying on putting it in a supplementary piece of legislation.

James Blessing: Or not putting it in any legislation whatsoever and just doing it as part of the notice from the Home Office.

Adrian Kennard: I think that is what it wants to do.

Q119 Suella Fernandes: When it comes to the issuing of retention notices, you understand that there will be an assessment whereby the Home Office is not going to issue them on all service providers. It takes into account the costs, the feasibility and the volume, and that is going to be informed by the Technical Advisory Board. There is a heavy element of discretion and consideration as to the practical implications. You appreciate that, do you not?

James Blessing: We appreciate that very much and it is the correct approach. The problem is that operational needs change, and the requirement for an ISP suddenly to get a notice because its particular group of customers is of interest to law enforcement means that we all, as service providers, have vaguely to sketch out how we would do that. When it is a nebulous "We are not quite sure what we are doing", you can do that, but you cannot plan to say, "I will make these changes to my network should I get that notice". As part of the Bill, we have gone from a situation where cost recovery was quite clearly stated as, "It is definite that you will get your cost recovery", to a slightly woollier version, which says that the Home Office "may" provide some cost recovery.

Suella Fernandes: But it is clear there is the duty to consult. It is very much a two-way process.

James Blessing: Yes.

Suella Fernandes: Lastly, there is also a power for you to appeal, whereby if it is disproportionate, whether on a practical or cost basis, the decision can be reviewed.

James Blessing: Again, that is absolutely fine. It is built into the system. We appreciate that, but, as someone who runs an ISP, the problem is that I have continually to assess threats to my business and threats to the operation of my network; and, at the moment, the Home Office turning up and saying, "You are going to have to start retaining this data", is classed as a threat. It is not that it might destroy our business, but it is going to take a lot of focus from my projects to provide service in rural areas or deploying the network in London. It is going to stop me concentrating on doing that part of the day job. There is absolutely no

method in the Bill for recovering any of those lost opportunity costs, so I have to put together a pot of resources on the side, just in case. If the Bill specified exactly what I had to do, I could probably get to the point where I could put it into a background level, have a plan and know exactly what I am going to do and how I get from there to there; and, when the Home Office turned up with a retention notice, the actual process of getting from the request to its being enabled would be a lot shorter as well, which, from an operational point of view, is beneficial.

Adrian Kennard: The key thing is that we do not have certainty in our business because we have this potential hanging over us. It is worth pointing out that the definitions in this Bill are very vague on who can be subject to these notices. It could cover schools, coffee shops providing wi-fi and it could cover businesses. They are all providing communications, albeit not as a business and not to the public, so for any business with any sort of IT department there is suddenly potential huge uncertainty over them with this Bill. It would be a lot clearer if the Home Office identified the operational requirements it has at the moment, which it has said are large ISPs, and the Bill pinned that down and said it has to be large communications providers.

Q120 Mr David Hanson: You will have heard the question I asked other colleagues earlier, which is, effectively, what your understanding of an Internet connection record is.

Adrian Kennard: The Home Office tried to explain it to us. Essentially, it was whatever you are ordered to collect, with huge scope for what that could be. We had discussions this morning when we were talking about event data, which seem to be about an event that does not have to have a place but has to have a time and at least one person and involve a communications service. If I have a conversation on the phone with a friend and say, "I am going down to the pub tomorrow", that is not an event, but if I say, "I am going down to the pub because they have really good wi-fi", that could count as event data because it relates to a communications service. It is so vague that, no, we do not know what it is.

James Blessing: The Bill itself does not make it clear. It is part of the concern we have raised repeatedly that, because it is not in the Bill, the code of practice has not been published and there is nothing else there, it is very much—

Mr David Hanson: Given that it is within a certain scope—we all roughly know, because the definitions on page 25 are what the Government think it should be, even if it is not nailed down yet—how easy do you think it is to do? If we said to you today that the Bill had gone through both Houses of Parliament and there was an implementation date of six months after it had gone through both Houses of Parliament, could you do it?

James Blessing: If you said that every telecommunications provider—it would cover an awful lot of people you did not realise it covered—was to be mandated that it must be able to record Internet connection records, it would be expensive. My network is not set up or designed in any shape or form to record this information, because I have as a business no need to do it; therefore, I would spend a lot of money on hardware. Six months is doable, but the other side of the coin is getting the data to law enforcement when it requests it in a format that makes sense for it. That is probably more work than installing new hardware across my network. I am going to have to send engineers to Cornwall and Aberdeen, but

that could be done. It is about the actual amount of other things where we collate all that information and then present it in a format that works.

Mr David Hanson: Adrian, you are a smaller provider. How does that impact on you?

Adrian Kennard: You said the definition is in the Bill.

Mr David Hanson: It is on page 25 in paragraph 44, where they say what they think an Internet connection record is.

Adrian Kennard: That does not really define it, I am sorry.

Mr David Hanson: That is the general broad scope.

James Blessing: That is the problem. To somebody who does not run a network, it is too vague a definition of what is wanted. When do you connect to the Internet? Where does the Internet start, for example? Is connecting to your home network connecting to the Internet or is it only when you leave that that it becomes an Internet connection record? Is your phone auto-updating its software with no intervention an Internet connection record? By definition, yes, it is. There are an awful lot of things that would have to be recorded that you do not realise happen in the background.

Adrian Kennard: I think you are referring to 47(6).

Mr David Hanson: I am referring to the background notes, the Explanatory Notes in broad terms, on page 25, saying what they are after. It is not the actual legislation, just the background notes.

Adrian Kennard: That is even worse.

James Blessing: That is the problem, because it is today's explanation, not tomorrow's explanation. Part of the reason that Internet connection records could be a problem is that, as the Bill is currently written, a Home Secretary in the future may decide to issue a notice saying that you must capture communications that happen over Skype, so you need to be able to identify which end-user talked to which end-user. It is not just that a Skype communication occurred, which we can do relatively straightforwardly, but which two end-users or multiple users were involved in that conversation. That goes into the dodgy territory of capturing third-party data because, as a service provider, I do not know which—

Q121 Mr David Hanson: Okay. We get the general idea. Given that the Government have established £170-odd million for this purpose, and it appears today that Virgin and BT are already planning to spend that amount, how much do you think it would cost you to meet the broad objectives that the Government are setting down?

Adrian Kennard: We are still stuck on the fact that it is a very broad objective, I am afraid. There are about three different levels of what we could be asked to do. If we already have a system that is logging some data for operational reasons, an email server that is logging emails that go through it, and we are keeping those for a few days to diagnose problems with the network, asking us to keep them for a year has some problems, but technically it is relatively straightforward and does not cost a fortune. There is a second level where we

might have equipment that can be convinced to create some logs but does not at the moment, and that is a bit more work. The third level, looking into the data as they pass through our network—where we are not the service provider for an email; where something is just passing through our network—is massively more expensive. It would double or triple our operational costs to have equipment that can look into the data as they pass through our network and extracts new information and logs it. The Bill has the scope to ask for that.

Mr David Hanson: I understand that you are a small provider. I do not know what that means in general terms, what your turnover is or how many contracts you have, but if the Government demanded that of you, how would you be able to deliver it, in terms of finance or—

James Blessing: Having vaguely sketched it—because I am a network engineer and it is sometimes an interesting exercise—in my bit of the business, which is the fixed line, not our parent company, our turnover is about £7 million. We have 40,000 or 50,000 end-users, so we are small in the grand scheme of things. You are looking in the order of £20 million to £30 million if I have to replace so much hardware on my network because it is not designed to do that; it does not have logging capability.

Mr David Hanson: Presumably if the Government do not facilitate your service doing it but do for BT, if I wished to be a child abuser, a criminal or a bank robber, I would use, with due respect, a smaller provider.

Adrian Kennard: That is a very specious argument, I am afraid. There are so many ways that anybody who is up to no good can bypass all this. They have no reason to go after a small provider. You cannot really trust that a small provider is not being monitored. It is possible that BT would be ordered to do some monitoring in the backhaul network that we, as a small provider, use. You cannot trust that monitoring is not going on somewhere in our service; it is just that we are not being asked to do it. Anyway, there is no need to. You just use any of the means to bypass this, such as Tor. At the moment even with things like iMessage you will not be able to see what is being communicated. Why would they bother trusting what a small provider says?

Q122 **Mr David Hanson:** The final point from me is in relation to access by the police. You will have heard other larger providers raise some points about access. How do you feel that would work in practice? Is what is suggested feasible? Do you have concerns about that or are you happy with the proposals?

Adrian Kennard: All this is about providing useful information to the police. The access is mostly a normal RIPA request, although there is the filtering facility and we still do not quite know what that will do. I am very concerned. We have experienced RIPA requests as an ISP, mostly about telephone numbers and some about Internet addresses. We have also experienced it as a victim of crime, when the police have been making requests of other providers to try to find our stolen equipment. Generally, we find that they struggle, even with modern communications. We had a case when one of our staff had to be an expert witness in a court case just to explain how phone numbers work, because they do not work in a simple way any more. My Bracknell phone number rings my mobile, my desk phone and my office phone. I seriously doubt, with that level of understanding, even with expert

help, that the police will be able to make use of any sort of Internet connection records. Even experts in the industry can have trouble keeping pace with the innovation and changing trends in usage. I do not think it is going to work well.

Mr David Hanson: Is the single point of contact officer—

Adrian Kennard: They are still not going to understand it enough.

James Blessing: Having dealt with a lot of single point of contact officers, they all have the right motives at heart and they are all trying to do their job. The problem is that they are policemen first, or other types of investigator. They do not necessarily understand the results. They also do not necessarily understand the implication of providing slightly wrong information. We have had a number of cases where the time zone was missing on a request; we get a request for a particular IP address asking who was using this IP address at this time and we reply saying, "At that time, it was that". Then they come back saying, "It could not possibly have been then". Then they work out that the time zone that they had recorded it in was in the US, and that was missing. It is little things like that. Until they do it for the first time, there are going to be a lot of mistakes. The filter may exacerbate that in the short term. Long term, it should make it better, but there is a massive requirement for training and support for the police and the single points of contact to be able to use it. There is an awful lot more work than has been put in and I do not see any funds in the Bill for that.

Adrian Kennard: I am also a bit concerned about how useless this information is going to be even when it is correct. One of the examples that has been touted by the National Crime Agency and the Home Office is about the possibility of a missing child and them wanting to get data about who the child was communicating with. They did not seem to realise that a mobile phone operator is going to be able to say, "Yes, that phone has been connected to Twitter 24 hours a day for six months since it was bought", but it does not tell you, "No, they looked on Twitter or they communicated with a friend on Facebook", because—

Mr David Hanson: It might do.

Adrian Kennard: No, it is going to tell you that Facebook has been connected 24 hours a day. That is how it works. Social media and messaging applications maintain a constant connection to the service provider. They do not wake up and say, "I have sent a message". You will find far more information about the missing child by asking their friends, because they tell everyone on social media. The ISP will not be able to tell that they chose to speak to someone at two o'clock.

James Blessing: On the comment I made before about when someone connects to the Internet, if you look at your phone now you will find it has updated your Facebook feed automatically in the background every few seconds. It is constantly doing it. You can tell that someone has a Facebook account, probably—

Adrian Kennard: But that is about it.

James Blessing: You do not know which Facebook account they are using, and you do not know whether they are actively using it or whether it is just that the software is installed and running. That is the best you are going to do in that situation.

Suella Fernandes: To follow up that point, you are aware that there have been very large-scale police operations that have been successful in large part because the law enforcement services had access to communications data or interception evidence. The Internet connection records can really help to provide a basis for further investigation, which can be critical.

James Blessing: Yes. I spent a couple of hours on Thursday morning helping a SPOC do some more research because they were not quite sure of what they had and they needed more evidence. I understand that completely. The problem with this is making sure we capture what is needed by law enforcement in a way that makes sense, so that it can interpret the information we provide securely and safely. It is not about not doing it at all. It is about asking what you actually need at the end of the day. The other problem you potentially are going to create is that, if you record all the records of every single connection that you are doing, stuff will be lost in the noise. You will start relying on data and say, "They were connected to there", when their phone might have been left in their bedroom turned on while they were somewhere the other side of town.

Q123 Suella Fernandes: I just wanted to make that point. A second question is about the security measures you use with the data that you have. Can you give us a bit of an idea of which mechanisms are effective for you?

James Blessing: As a company, we take credit cards, and there is a standard that we have to follow for that, which basically means the information is stored in an encrypted database with multiple levels of firewall protection. As far as we are concerned, if we were to do this, I would put the same level in place. I would do some checking. Part of the reason the filter is a concern is that you have to give third-party access to it, and it might need some engineering work to make sure that only trusted parties can access it, but that is a different issue.

Suella Fernandes: You say that firewalls and personal vetting systems are sufficient.

Matt Warman: Very briefly, it seems that a lot of what you have been saying is that there is a whole load of stuff that we may or may not need to record—some of that stuff about "When is your phone connected to Facebook?" All that I absolutely understand, but once we have nailed down the definitions that ceases to be your problem.

James Blessing: Yes. Nail down the definitions and everyone starts going, "Right, okay, now I can work out how to deal with it".

Lord Strasburger: I want to clarify Ms Fernandes's question. I presume she was referring historically to communications data derived from telecommunications rather than from the Internet. What you are saying—the view you are expressing, if I am hearing you correctly—is that the efficacy of the Internet communications data that are going to derive from Internet connection records is doubtful, as opposed to telephone communications data.

Adrian Kennard: Telephone communication is very clear-cut; it is the building block of the telephone network that telephone calls are made and everyone understands the concept and it is very clear. The Internet is not like that. Devices are constantly talking, constantly communicating with lots of different services all the time. Connections can stay running for

days, months or years, and that is one connection. The usefulness of this is much more limited, with a lot more noise. It could be misused easily. It is very easy for someone to appear to be accessing services they have never heard of. I did a blog post today, and anyone who reads it will find they have accessed Pornhub because there is a tiny one-pixel image in the corner. They do not know that, but it will appear on the Internet connection record if they access my blog. That was deliberate, but there could be lots of things on websites, advertising networks and so on, that will create all sorts of misleading and confusing data even without someone trying to be misleading. As I understand it, in Denmark they had nearly a decade of trying to capture sessions on the Internet and abandoned it because they found it not to be very useful for law enforcement.

The Chairman: Ms Fernandes, did you want to come back on that other one?

Suella Fernandes: No. I meant how people are sending emails, what they are sending on the Internet.

The Chairman: I meant on the Information Commissioner.

Suella Fernandes: You are right; it was to follow up Lord Strasburger's presumption about what I meant in my question. I lost my train of thought. The question I wanted to ask initially was whether you think that firewalls and personal vetting services are sufficient for maintaining security.

James Blessing: Let us get this right. If operated according to design by the right people in the right way, yes. The difficulty is that operational procedures can drift away from perfect. It would not surprise me if there was a breach of the data stored in an Internet connection record at some point. It is not a question of if; it is a question of when. There will be a breach.

Adrian Kennard: Bear in mind that even the NSA, which has huge resources, had Snowden. It does not matter how well we do this, somehow someone will lose data; they will be breached and it will potentially be sensitive personal information.

James Blessing: As an example, the Home Secretary has possibly made herself a target for people who want to show that this is a bad thing to do; they may well try to go after her home service provider because they think that is a good thing to do.

Q124 Stuart C McDonald: You referred a couple of times in passing to filter requests. What is your understanding about how these are going to work, and what concerns would you have about their operation?

James Blessing: In theory, the filter is being described as a way of restricting the information recovered. That means that an automated system must be doing the requesting of the data capture from the service provider and then presenting them to an individual. That means we have to allow third-party access to our systems, which is a potential risk. In theory, it would mean that the data was less open to fishing because you are only getting back specific results, but potentially there is a whole new construction of requests that people could start making, saying, "Who has visited Pornhub recently?" and Adrian's blog, and then putting that together, because it might be an interesting subset of

people to go and do something else with. In some ways it is a good thing and in some ways it is a concern, because, again, the details are very limited.

Stuart C McDonald: It is the Home Office that would build the filter; is that right?

Adrian Kennard: I do not think it is specified.

James Blessing: Again, part of the problem is that it is not clear who operates which bit of the filter and how the filter would work. As far as I can tell from the information provided so far, it seems to be implying some sort of API access.

Adrian Kennard: Automated.

James Blessing: It is an automated access. Basically, a request comes in and it returns that information. How that happens in real life is not clear.

Q125 Lord Henley: Can I turn to Clause 189 and the ability of the Home Secretary to impose certain conditions on relevant operators and that these would come in the form of technical capability notices? I would like to hear what your views are on the ability of the Home Secretary to impose such a notice. How do you think your customers are going to react?

Adrian Kennard: My biggest concern is the removal of protection on communications. This comes down to the whole issue with iMessage, to some extent, in that it is end-to-end encryption at the moment. If providers are required, even secretly, to remove that protection, it removes all trust in those providers if they are offering a secure communications service but at any time they could be subject to an order that makes it not secure. That is a reason for companies to avoid being based in the UK and for customers to avoid UK companies. Encryption is a good thing; it is what keeps us safe from the very real threat of cybercriminals. If you got every communications provider in the UK, and even every foreign communications provider, to have this capability and to remove the protection they have provided, that still does not stop people, including criminals, communicating secretly. There are applications that do the encryption for you on your own machine when you send messages so that the provider cannot remove it. It is even possible to send messages that are completely secret—GCHQ could not get the information from those messages ever—just using pen, paper and dice. You could ban all computers and it would still be possible for people to communicate secretly. It is undermining trust and not solving any problems to tell operators they have to remove protections.

James Blessing: Most of the stuff is covered. The issue again is that it is not the Home Secretary who would be requesting that. It would be law enforcement because it needed to do something, which always comes down to this: most service providers are willing to help law enforcement because, at the end of the day, we are part of a wider society. Forcing someone to go and break something tends to mean there has been a disagreement about doing something in the first place, and that is not a good place be to be.

Adrian Kennard: I have one other concern to do with the definition of communications provider. I have another hat today. I am a manufacturer, a UK business, making equipment that we sell round the world—a firewall router that would go in a small office. I am very concerned that there is the possibility that we could be asked to put in back doors or

remove encryption as part of this. I think we would have to move the business out of the UK if the Bill goes through as it is at the moment.

Q126 Lord Henley: Now we turn to oversight and the proposed Investigatory Powers Commissioner. How do you see your relationship with him or her, and what changes would be appropriate when that office is created?

James Blessing: It is good that additional oversight is being created and put in place. That is always a useful thing to have. It is not clear from the Bill how independent a voice that person would have considering they are going to be appointed by the Home Office, pretty much, and they would be a judge. I am a bit sceptical that they would be as independent as their job title would lead you to believe.

Adrian Kennard: Yes. I have similar concerns.

Lord Henley: Finally, my Lord Chairman, I have one other question for clarity. I think it was Mr Blessing who implied that the costs imposed by the Bill, if enacted, could be such that his business would have to spend something of the order of four times your annual turnover.

James Blessing: Yes. Basically, the reason for that is that we have grown over time from a small organisation. We build the network small and then grow it, so there are no logical places within our network to do all the stuff that is required. We would have to go through replacing lots of pieces of hardware and upgrading them and their capabilities.

Lord Henley: Would that same figure, a factor of four, be as true both for small providers such as yourself and your membership as for some of the larger ones?

Adrian Kennard: It is difficult.

James Blessing: It is difficult. There are certain service providers where, because of their business model and the way they have built their network, it would be easy to do and it would not cost that much, but there are others in our situation where it would cost that. There are probably others where the multiplier is even higher. It will be variable because every network is different.

Lord Henley: The figure you were giving was one from your own experience with your own business.

James Blessing: Yes.

Lord Henley: It would not necessarily be true of all your members, but it might be higher or lower.

Adrian Kennard: Our business is different yet again. As James was saying, every ISP does things differently; it has different networks and will have different costs in doing things. In our business we make those FireBrick products and sell them to ISPs and use them in our network. It is entirely our own R&D in the UK and we have spent millions developing it. If we now have to change that to do different things, it could cost millions, or we scrap all our own work and buy in third-party kit, which would also cost millions. We would have to make major changes to do that.

Matt Warman: You talked about your fear that the Bill might ask companies to stop end-to-end encryption or that it might ask for back doors to be inserted. We have had the Home Office in front of the Committee saying that is not the case. The Home Secretary has said that on the Floor of the House. Are you saying that you do not believe them when they say that—

Adrian Kennard: No. But put it in the Bill if that is the case. It is as simple as that.

Matt Warman: The end of my question is whether you would simply like more clarity.

James Blessing: The issue is not the current Home Secretary or Home Office. That is the problem. It is that you have put it in the Bill; it is there. There are two things. It is in the Bill and therefore we are looking at it saying, "Technically, someone could do that". More importantly, someone outside the UK who trades with the UK will look at the Bill and say, "That technically says that they could do this".

Adrian Kennard: And "I am not going to deal with them".

James Blessing: I have two choices: this company in the UK and this other one outside, and I am a bit worried about that, so I will use the other company instead.

Adrian Kennard: We have already seen how putting too much scope in a Bill can be abused, with councils using RIPA to spot people going to a school outside their catchment area. I am sure the council thought, "We have got this power and we would be negligent not to use it". I suspect future Governments, Home Secretaries and Secretaries of State might well say, "We have got this power and we should be using it". Anything that is possible could happen. It is worrying.

The Chairman: On that very interesting note, thank you both very much. It was a very useful session, very informative. Thanks very much for coming along.

Baroness Jones of Moulsecoomb (QQ 174-185)

Evidence heard in public Questions 174-185

Oral Evidence

Taken before the Joint Committee

on Wednesday 16 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Lord Butler of Brockwell, Bishop of Chester, Lord Strasburger.

Witness: **Baroness Jones of Moulsecoomb**, gave evidence.

Q174 The Chairman: Mr Davis, Baroness Jones, we are very grateful for your coming along to the Committee. We think that you have some very interesting things to say about this Bill, and I will kick off by asking a question that is so general you can make a general statement before individual questions. The same question, first, perhaps to Mr Davis and then to Baroness Jones: is this Bill necessary, and to what extent does it address your concerns, if it does so at all, about legislation in this area?

David Davis: Thank you for the welcome, Mr Chairman. It was either you or the Berlin Christmas market. You won this time, so I have just leapt off a plane. Is it necessary? Yes, it is necessary. There is no doubt that we need a new Bill. It is taking over, if you take David Anderson's count, something like 66 statutory mechanisms for various forms of interception, data gathering and so on, many of them based on bad laws. RIPA is a bad law. I am sure some of your witnesses have told you that already, but it is very badly drafted. I can come back to that in a minute. It is also taking over laws that are used in ways that I am quite sure Parliament did not intend.

I would have hoped that it would have consolidated all the electronic surveillance laws into one area. It has not done that, so its first failing is that it has not concluded that. You have just had witnesses from law enforcement agencies, have you not? The police Act is still effective. IMSI-catchers, the devices that block and intercept mobile phones, for example, would go around this, and that is part of the propensity to expand on the part of the agencies. All agencies in the world expand their powers, and this encourages it.

It is good for another reason and that is, in a consolidated form, that it will be possible not to future-proof it but to future-adapt it. A lot of the argument that you get from the agencies is that we have to make this future-proof, which tends to be an argument for making things more general, open and loose. That is a bad idea, but we are probably going to have to get into the habit of probably having one of these Acts every Parliament anyway—just as we have a Finance Act every year and a Companies Act every year or two—because of the rate of change of technology.

Does it meet all my concerns? You would be surprised if I said yes, would you not? The answer is no. On authorisation, which again I am sure we will come back to, it is a missed opportunity, because a new consensus was developing on judicial authorisation. They have missed that. It is certainly not what somebody described as world-leading. If I had to pick the world-leading country in this area, I would probably pick the United States for where it is arriving at now rather than us. I do not think that the double lock is very good. It claims to introduce one new power, but in practice you have internet connection records as well as effective recognition or avowal of bulk equipment interference, bulk personal data sets, bulk data and even thematic warrants. Although they were not formally approved by Parliament, somehow they were invented out of RIPA. There are a whole series of areas where it is weak, but broadly speaking we have to have a Bill along these lines.

The Chairman: Baroness Jones, if I can just repeat the question, is the Bill necessary, and to what extent does it address any concerns you might have about legislation in this area?

Baroness Jones of Moulsecoomb: Lord Chairman, thank you very much. I am missing our team Christmas do and they are all in the pub waiting for me, so I am sure you will understand if I speak quickly. I suppose you could say it is necessary, because times are moving on. Obviously we now have huge ability in surveillance, and so some sort of way of containing it and monitoring it is incredibly important. The majority of powers in here are new.

My concern is twofold. First, this is covering what has been done up to now, because the laws that have existed so far have been broken and abused many times by security agencies and by the Met. I have quite a list, which perhaps I could give you subsequently. I am concerned that there is a good operational case for this and that they really understand how to use the powers. I am concerned that they are going to use these powers to spy on people who are holding them to account, because this is what has happened already. Security agencies and the Met Police have used powers that they do not have to spy on people, for example Doreen Lawrence, who tried to hold the police to account. Mark Thomas, who is a comedian, tries to hold the state to account. There are five journalists who have been spied on so far, and even I had for 10 years, when I was an elected person sitting on a police authority, a file on me in the Met's domestic extremist database, which is fairly outrageous. I am quite clear; my life is quite public and there was nothing to hide, so I do not feel that I was intruded upon, but at the same time what a terrible waste of time and resources, and it was not just unnecessary but unlawful at that stage.

There is also the fact that Snowden has told us that GCHQ intercepts 50 billion internet communications a day. Now, that is an astonishing amount of data coming in. Over the years, I have asked the Met Police how many databases they have to get an idea of how much information is coming in. They could not tell me to the nearest hundred or to the nearest thousand how many databases they had, so we are looking at something that is potentially very complicated. There is a vast amount of information coming in. Do they have the skills to deal with it?

Q175 Suella Fernandes: I have one general question. Do you agree that the Bill before us today represents progress compared with the Draft Communications Data Bill in 2012?

Baroness Jones of Moulsecoomb: I would say that there are things in here that I am deeply unhappy about.

Suella Fernandes: How does that compare with what we last saw in 2012, in that now local authorities do not have any powers? That is a movement from 2012, is it not?

David Davis: There are marginal improvements. There is no doubt about that. As I said, the fact that there is a single Bill of itself is an improvement, but it is a long way short of what it should be. One of the things that worries me, Chairman, and I hope you will take this in the spirit it is intended, is that it is going to be incredibly difficult for you as a Committee to deal with this Bill in the time available. It is an enormous Bill, particularly when you take on board all the newly avowed powers. They are not new powers in the sense of being used, but they are new for Parliament. Assessing whether they are right or wrong, effective or ineffective and proportionate or not an erosion of privacy is going to be incredibly difficult, and in this business speed is the enemy of wisdom, so it is quite difficult.

My comment is that they are granny footsteps towards a better position. We must not miss the opportunity to get this right, both from the point of view of protecting the values that we are supposed to protect and, on the other hand, making the agencies more effective. They are behaving in a very different way from some of our allies, who are arguably more effective.

Baroness Jones of Moulsecoomb: The Government appeared to make some concessions, because there was quite a furore about this. For example, they brought in judicial review, but the judicial review is very light and in fact can be completely ignored. If Ministers decide there is some sense of urgency, they can go around the judges altogether, despite the fact that the Royal Courts of Justice has a judge on duty 24 hours a day. They appeared as concessions but they do not go far enough.

Q176 Lord Butler of Brockwell: If I may follow up that point, when you say that the Government could ignore the judges completely, are you referring to it being within five days if it is a matter of urgency?

Baroness Jones of Moulsecoomb: Yes.

Lord Butler of Brockwell: If I may respectfully say so, surely that is not ignoring the judges completely.

Baroness Jones of Moulsecoomb: They can bypass them.

Lord Butler of Brockwell: It is for five days.

Baroness Jones of Moulsecoomb: Perhaps I can talk about the volume of stuff that is coming in. The Prime Minister will be told if there is a warrant for people like us, for example—privileged people. For me, those are the people we are going to have to be very concerned about. These are the people who get whistleblowers coming to them, whether journalists, ministers of religion, parliamentarians or whoever. The Prime Minister will be notified of a warrant but does not necessarily have the right to reject that. The warrant will go to a judge. Am I saying this wrong? The judge or the commissioner only reviews it. The judge is not able to say yes or no. The Minister can then take it to the investigatory powers

commissioner, who can overrule the initial commissioner, so there are lots of ways in which these things can be pushed through.

Lord Butler of Brockwell: I will not continue this, but the investigatory powers commissioner is of course a judge.

Baroness Jones of Moulsecoomb: Yes.

David Davis: Lord Butler, can I give you my view of this, which is not the same? I do not view the accelerated procedure as a necessary bypass. It is going to have to be refined in some ways, but of course there are circumstances in which fast decisions have to be made. In the London/Glasgow bombings, for example, telephone data was very important and you had to make a decision very quickly indeed—maybe in minutes. You have to have a procedure like that. There is of course, in my view, a need to keep a very close eye on it and maybe publish how many times that is triggered every year. Frankly, make it plain to an officer who uses that procedure that if he is in the wrong there will be a mandatory warning on his record, but I do not see it as a bypass. I do not share that concern.

Q177 Lord Butler of Brockwell: Thank you very much. Could I get on to bulk interception? Are you satisfied, and I may ask each of you in turn, that the operational case has been made for bulk interception, bulk acquisition of the collection of communications data and bulk equipment interference? Perhaps I could use my second bit of ammunition before I ask you this question. This is a matter that David Anderson looked at and said he was satisfied that those powers were necessary. Do you agree with him?

David Davis: I do not entirely. Let us take bulk interception first. It is insufficiently narrowly defined for foreign for example. Charles Farr, when he gave evidence in 2012, I think, said that the selectors on the bulk intercept data would obviously pick up British-to-foreign intercepts and would treat accessing Facebook, Twitter or any foreign platform as appropriate for this. That seems to me to be too broad and that they have not made the case to justify it being that broad. If we are talking about bulk intercept of a fibre optic going through Cyprus to Pakistan, I am going to be more relaxed about it. That is the first thing.

Your second point was about the bulk acquisition of communications data. The best model here is America's. They basically recoiled from that after the President's panel had a really deep look at it. There was a previous director of national intelligence and very serious counterterrorism lawyers on the panel. They looked at it and came to the conclusion that what they were doing was simply not worth it. We would have to make a much stronger case to come back on that.

On bulk equipment interference, individual targeted equipment interference is obviously a necessity, particularly in this day of encryption. It is one way of getting around encryption and probably the most effective, but bulk interference worries me a lot. It is a very serious intrusion of everybody's privacy. We know already that one of the agencies has effectively suborned very large numbers of SIM cards—in the millions. That sort of thing worries me. Apart from the direct assault on individuals' privacy by the state, it would undermine the integrity of their own personal security to anybody else—to a blackmailer or to somebody trying to intercept them.

One group that you did not mention which I am going to raise because it almost falls off the tongue is bulk personal data sets. It is avowed, but there is very little in here. It is not for me to give the Committee advice, but if I was going to point at something that needs to be looked at, I would look very hard at that as well. This has explicitly been disavowed as an approach by the Americans and others, and it really is completely antagonistic to the things that the current Government and the previous Government set their face against. In the identity card arguments, the primary argument about the identity card was not about carrying a plastic card but about the existence of a central national database of personal data on every citizen, and it sounds to me as though we have had that since certainly 2005 and possibly 2001, which is what shocked Mr Clegg. There is a very large number of areas where other people have found that these are very bad ideas and do not work and have recoiled from them, sometimes even the agencies without external intervention, on cost-effectiveness grounds. We need to have a much tougher, more challenging attack on this if we are going to justify it.

Lord Butler of Brockwell: Just on that last point about bulk personal data, are you reassured by the fact that under the Bill this would now require a warrant that would have to be endorsed by a judge?

David Davis: That is an improvement, but on the very holding of this, I do not know whether you can see the data sets that they have. We are pretty sure, at least reporting on the register today, that they have all the communications data. They have flight data. They almost certainly gave financial data. They may well have ANPR data. This is very intrusive information for a state to hold. We have been having arguments for the last 10 years about whether we should have a central database for ID cards, or whether we should have communications data, hence the stalling of the so-called snooper's charter, when in fact this has existed throughout that. One thing that I would hope the Committee would come to a view on is what is in this, because there are arguments that there are hundreds of data sets here per person, which is really very serious. Yes, you are right that warranting is good, but frankly the extent to which much of this database should exist is very debateable.

Baroness Jones of Moulsecoomb: There are also, of course, medical records and financial asset records, and so on, in those data sets. It is a very wide scope.

Lord Butler of Brockwell: Baroness Jones, do you want to add anything on bulk collection?

Baroness Jones of Moulsecoomb: The bulk collection of domestic phone records, of course, has been proved to be ineffective in the States under a similar power. The President's review group said that it was not essential to preventing attacks. The Privacy and Civil Liberties Oversight Board concluded that it had not identified a single instance involving a threat to the United States from that sort of collection, so I would argue that it is of very limited value.

Q178 Victoria Atkins: Just on that point, you have listed all sorts of information. What is the basis for asserting that those are sets of information held by the authorities? How do you know? You have told us that with some confidence.

David Davis: Some of it has been around. The place to look is an organisation that used to be called GTAC—probably in your day, Chairman. It is now NTAC, the National Technical

Assistance Centre, based at Thames House. It has already been recognised in public by Ministers that intercept data is there. These are the people who handle most of the requests from all the agencies. It has been in the public domain that there is a financial set, which I assume is credit cards and bank records, because GCHQ has a title for it: FININT. Flights we know about. The question was about the rest. As to whether or not they have ANPR, it would be very surprising if they have this and have not put ANPR in it, for example. If I were going to build a database like this, given their purpose, that is what I would do. It needs to be answered. One of the things that has been said for a start by a number of security journalists, who know their way around this, is that they think there are hundreds of data sets—not one, not five.

Victoria Atkins: Do you worry, in listing these data sets as you just have, that you have given some very helpful information to serious organised crime gangs, terrorists and others?

David Davis: In that case, I would arrest Malcolm Rifkind, because he drew it to the public record in March last year. It was only when that was done that this was put under the intelligence commissioner's oversight. Until then, there was no oversight whatever. I am afraid that in a democracy it is necessary to look at what you are doing, and you can only do that by discussing it.

Baroness Jones of Moulsecoomb: The scope very definitely has to be well defined, which it is not at the moment. There is also the fact that once you have warrants for this bulk information, access is much freer. Once you have it, there are stacks of stuff in there that you can freely search whenever you have an appropriate moment. It is not just a one-off search.

Victoria Atkins: I have a question to both of you: what is the correct balance between the democratic accountability of Ministers and the independent oversight of judges in the authorisation of warrants? Does the draft Bill get this right?

Baroness Jones of Moulsecoomb: I would like to have seen a little more of the judges being able to look at the legal aspects of whether or not to grant a warrant. That is lacking at the moment. Politicians vary enormously in their skills and may not be the best people to have that sort of last word or ruling.

David Davis: Our approach to this and that of some of the Commonwealth countries is based on the royal prerogative concept of government. That it adds accountability I would dispute absolutely. Jack Straw always used to say that when you are in trouble, the safest place to be is the Dispatch Box of the House of Commons. That is certainly true when it is a terrorist event. I was the opposition spokesman who responded to Charles Clarke on the day of the 7/7 attack, and you can be quite sure that the aim of the Opposition at that point was not to embarrass the Government; it was to show solidarity against an outsider. That always happens. You may remember Gibraltar, when the Labour Party was very supportive. Even though there were some doubts on the day, they were very supportive. Even a few weeks ago when we had the drone attack, there were some differences between the Prime Minister's approach in the Chamber and what was written to the United Nations, but nobody went for that, because we and the public take a view on this.

Secondly, when it comes to warrants, it is very often illegal for the Minister to talk about it publicly anyway. I suspect that you have had some Ministers in on this. It is legally forbidden to talk about it. The pressure on a Minister to be accountable is near zero. If you look in *Hansard*, you will find a number of Parliamentary Questions from me asking the mundane question: what law, what statute, was this done under? I got the answer that we never comment on security matters, so we do not even know. That is how accountable it is; we do not even get an answer about which statute is being used.

First, the accountability argument is a chimera. It is a problem for countries such as the States, which takes a very different view of the royal prerogative than we do, obviously given their foundation. Many of them view the idea of ministerial approval as being rather flawed.

To take up the Baroness's point about skill, we are very unusual at the moment. We have a competent Home Secretary who has been there for over five years. When I was shadow Home Secretary for five years, I had four opponents, one after another—Blunkett, Clarke, Reid and Smith. The typical tenure of a Home Secretary is about two and a half years: a year getting into the job, a year understanding it, and then they are on their way. What do they do? What does this warrantry process consist of? There were 2,345 warrants last year: 2,700-odd in total, but 2,345 signed by the Home Secretary. That is about nine a day on a working day, if you assume that she signs one or two before going to church in a hurry on Sunday. It is about nine a day on working days, 50 weeks a year. That is not long enough to do this. Fifteen or 20 years ago, there were about 1,000 a year. I spoke to one of the Home Secretaries who did it then. He said that even 1,000 a year was too many. You never got enough information to make a judgment; you got a précis of the case. You cannot make a judgment on something as intrusive as this on a précis. You get no chance to do much cross-questioning.

Victoria Atkins: Which Home Secretary is this?

David Davis: You will have to call him yourself.

Victoria Atkins: I cannot if you have not told me.

David Davis: I am not going to tell you without his permission.

Victoria Atkins: This is hearsay.

David Davis: No, I am just telling you. You can work it out if you try a little. One thousand a year is what they did then. It is now at 2,500 and going up. From that point of view, compare that against using a judge or a panel of judges. First, they are more expert. They are in the job for a long time. Look at the example of SIAC. If we were smart about it, we could do what the Americans do and effectively put up a special advocate to challenge and make sure that the public interest is maintained. That is the way to do it. That is much more effective than this way. I am afraid that this way will improve it slightly, but it misses the optimum outcome.

Victoria Atkins: A simple question: who judges the judges?

David Davis: We are going to have a whole new procedure in place of other judges. Most judicial systems have a structure to them where things are reviewed further up. That is what has happened here. That putting-together of the overarching commissioners, by the way, is a very good bit of the Bill. That is straight out of Anderson, and Anderson was exactly right.

Baroness Jones of Moulsecoomb: What we are talking about here is high-level authorisation. I heard the police officers talking earlier about who was going to be able to give such authorisations, and it can in fact be at a much lower level. A detective sergeant was found last year giving out authorisations.

Victoria Atkins: Was that of intercept warrants?

Baroness Jones of Moulsecoomb: Yes.

Victoria Atkins: That is not my understanding.

Baroness Jones of Moulsecoomb: No, but it is an indication of where a structure can break down, because that detective sergeant did not even know that journalists had a duty and a right to protect their sources. Things can decay in use, which is my experience of the Met Police.

Victoria Atkins: Is the proposed procedure for urgent applications for warrants for intercept, part 1 of RIPA, appropriate?

David Davis: We have different views on this, as is apparent from the answer to Lord Butler earlier. I think it is broadly appropriate. Five days is quite a long time, even in the Civil Service, so it could be shorter than that, but as I said we should publish the number of times we use these every year. We should establish some clear criteria. Obviously in an imminent life and death situation it is a no-brainer, but there are a few others that may not be quite so clear-cut. The London/Glasgow bombing is one example. It was not imminent life or death; it was 12 hours or whatever it was before the attack, but those hours were slipping away. They needed to move quickly with what information they had, and it is very hard to legislate for that, so you have to allow a little tolerance in the urgency. There may also be some circumstances in which there is the possibility of losing information. Information is only available for a very short period. Just those three completely different criteria demonstrate that urgency is rather hard to define. It is very easy to recognise and hard to define, but we could certainly write a statute to cover that.

The Chairman: What you are saying, Mr Davis, is that with regard to the urgency, in your previous answer to Lord Butler, you would advocate first of all that the time of five days is shortened and, secondly, that there might be some special investigatory process for those urgent ones to ensure that they have been dealt with properly, as urgent.

David Davis: That is right. The other thing that I did not mention, of course, is that under my preferred approach, which is a permanent on-duty judge, you are going to have less of a problem most of the time, unless we are happy to wake up the Home Secretary every moment of the day and night. You would have a 24-hour panel. You would still need a process, but it is the sort of thing that I would only expect to be used relatively few times a year—single to double figures, no more than that.

Suella Fernandes: Just to follow up on this, have either of you ever authorised any warrants?

David Davis: I have refused to authorise one.

Suella Fernandes: Is that to be read that you have not been involved directly with any authorisation of warrants in your roles?

David Davis: Yes, except for the one occasion.

Q179 Stuart C McDonald: You have both made pretty clear your views on having this double lock of first a politician and then a judge, but assuming that we retain that double lock, what standard of review is appropriate?

David Davis: This has been quite an area of argument, of course, because the Bill states judicial review standards. Of course, that leads you down all sorts of routes. If you take Wednesbury standards, which is a sort of procedural, "the Minister must have been out of his head", clearly that is not good enough, as often as that may happen. The real standard, and why I wonder why they put in judicial review standards, is that basically it should be a judgment about necessity and proportionality. That is what should be there. There have been debates. Have you had David Pannick in front of you?

The Chairman: No, we have not.

David Davis: You have had people quoting him, I am sure. He says that in these cases it is not really Wednesbury; it really is proportionate when it involves human rights. He was citing cases where people's liberty was at risk, basically in SIAC and so on, which is quite serious. In the very next paragraph of his article, he talks about how judges do not like to overrule the Executive, the Ministers, particularly when it is a matter of national security. You have a balance both ways. One of the things that this Bill needs is absolutely explicit explanation of how the judge will make the decision so that there is no doubt about it. I also think there is a problem about the judge going immediately after the Home Secretary. It is a pretty brave judge who turns over a Home Secretary.

Baroness Jones of Moulsecoomb: I feel more or less the same way.

Stuart C McDonald: The two former Secretaries of State who we had before us were both horrified at the notion that you would have detailed or intensive scrutiny of decisions involving things like life and death, but you seem to be the opposite way round: these are the ones that would require a higher standard of scrutiny from judges.

David Davis: Can you say that again? What did they say to you?

Stuart C McDonald: They seemed to be aghast at any sort of notion that a judge would engage in a very strict and detailed scrutiny of decisions on imminent matters of life and death, for example.

Baroness Jones of Moulsecoomb: Judges are trained to assess evidence and to assess whether or not a course of action is appropriate. I would argue that that surely is a better route.

Stuart C McDonald: You would essentially want the judge to make a decision fresh themselves, based on the same evidence. It is as simple as that.

David Davis: If you really had to have a double lock, which is a silly title for it—it is more like a loose latchkey—I would put the judge first.

Q180 Suella Fernandes: You have mentioned David Pannick's article, but we have heard evidence from Lord Judge, who is the former Lord Chief Justice and head of the judiciary, and Sir Stanley Burnton, who is the Interception of Communications Commissioner. They both, as senior judges, have experience in this area of law. They have both said that the judicial review test here necessarily imports the test of necessity and proportionality, and that it is the right test that strikes the right balance. Are you disagreeing with them?

David Davis: Yes, I am. Let me give you an example of why, from the intelligence area but not from intercept. In the case of Binyam Mohamed, when the Court of Appeal was considering whether or not to put into the public domain a five-line summary—nothing harder than that—of the fact that the British state had likely been colluding in torture, it took them months to get round to doing it because they were so reticent about overturning the opinion of a Foreign Secretary. They did it eventually only when an American court published the hard data. Even then, they redacted from their own judgment comments about the agencies. Now, that is a very good parable, but it is not the only one of judges being very cautious, and you can understand why, about critiquing an existing government decision, an existing Secretary of State's decision, particularly quickly and particularly with national security. They are just as susceptible. They are not saints. Judges are as variable as Ministers in some respects, but they are human. They do not want to be the person who says, "No, you cannot do that", and then somebody gets killed. After all, at the end of the day, that is the core question in all this.

Suella Fernandes: Do you not think that, for transparency purposes, if there is a threat of an imminent attack, for accountability, legitimacy and reassurance for the public it is the Home Secretary, a Minister, who will need to face members of the public on making a decision, not a judge behind closed doors.

David Davis: The Americans do not find that.

Suella Fernandes: We are not America.

David Davis: No, I am giving you an example of where it does not happen. The Americans do not find that. Nor have I seen a single example in my time in the House of a Minister being held to account for a failure of the services—just the reverse. Go back and look at 7/7. The Opposition very carefully, some may remember, did not call for an inquiry into that. Why? The actions of the political body, in toto, were to act in solidarity, not to challenge each other at that point. The accountability argument does not stand up. I do not think that the public are even aware, most of the time, of individual warrantry.

Also, we are talking about terrorism. Let us be clear about this, because I may have a different view from other members of this Committee: terrorism is not a war, it is a crime. By calling it a war, we give advantage to the other side. It is a crime. We do not require Ministers to sign off warrants on other crimes. I do not see why the public would necessarily

expect them to sign them off on this. What the public wants is a safer outcome with the minimum of intrusion into their lives. They will not be worried about the procedure.

Baroness Jones of Moulsecoomb: There is also the fact that it is very hard for any Home Secretary or any Minister to say no to the security services, if they are saying, "You must do it. You have no choice". I would have thought it would be far better to rely on a judge having looked at the evidence and assessed it properly.

David Davis: I do not necessarily agree with that, to be honest. The current Home Secretary does say no to some.

Baroness Jones of Moulsecoomb: I would agree that Theresa May is doing a splendid job.

David Davis: That was not the point that I was making. She does say no to some. The one I am unwilling to name, but I will ask if he wants to name himself, certainly said no to some, more than some, so I do think that they take it seriously, but I just think that they are making a decision on a précis. This is a life-changing decision, and it is sometimes a life-saving decision, on the basis of a précis.

Baroness Jones of Moulsecoomb: I did not say they would not. I just said it is hard.

Victoria Atkins: Mr Davis, you said that it would be a brave judge who stood up to the Home Secretary. Does that not undermine your argument that judges should be solely responsible for this process, because if they are not brave enough to stand up to the Home Secretary, the Foreign Secretary or the Northern Ireland Secretary, one wonders how much they are adding to the whole process?

David Davis: They are good and poor procedures and this, in my view, is a poor procedure. That is the point. What pressures are built into the procedure? You design judicial procedures to give a fair outcome, and you should design these procedures to give the best outcome, the optimum judgment, from the judge, and this is not the way to do it.

Q181 Lord Strasburger: I have a slight change of tack. Some jurisdictions have a method for informing those who have been subject to surveillance after the event, after the case has concluded, thereby giving them an opportunity to seek redress, perhaps in our case through the IPT or perhaps through normal courts. Do you have a view on that?

David Davis: Yes. In the countries that do that, it is quite constrained. Obviously if somebody is still subject to investigation, it is never going to happen. If there is an ongoing case still, it is never going to happen, and even if it is the next-door neighbour it is not going to happen. Nevertheless, the existence of such a procedure is a very good discipline on the agencies themselves and on the people making the decisions, because that way mistakes will out eventually. Frankly out of all of them, only a relatively small number are ever declared, but the existence of the procedure is quite good.

Q182 Shabana Mahmood: I just wanted to return to this whole politicians against judges argument. Is the whole point not about political accountability—the "who judges the judges" question? The politician in this scenario is trying to achieve something different, which is a unique threat, a unique capacity for scale of death and slaughter, and making a decision very quickly. The judges are fundamentally doing something very different, which their training

teaches them to do. It is fundamentally different from the politician's job. Why do you think that political accountability should go from a process that is only about judges simply applying the letter of the law, making a judgment on the day, but not worrying about any other of the ramifications that that might have for our national security?

David Davis: I think I have said twice now, so forgive me, Chairman, if I am repeating myself for the third time, that the operation of the House of Commons in particular, in terms of effecting accountability, and indeed the operation of the British media, because the British media also go shoulder to shoulder when this sort of attack happens, is not one that delivers conventional accountability. Let us imagine for a second that we had a Spanish situation. One reason why, when I was shadow Home Secretary, the Conservative Party redesigned our approach to what we would do in the event of a terrorist attack was because of what happened in Spain. As it happened at the general election in Spain, I thought it might happen at the general election in Britain, so I thought, "This is not going to happen in Britain".

Let us imagine for a second that it did and that we tore into the Home Secretary of the day because the agency had fallen down on this, that and the other. The truth of the matter is that they did fall down on some things. I am not going to replicate them here, but they are easy to look up. The last thing we would be worried about is who signed off the warrant. It would be what did not work. What did not work? We know what did not work. They had information about Mohammad Sidique Khan. They had a photograph, and they cut it the wrong way and sent it around in an unrecognisable form. This procedure does not add to the accountability. It seriously undermines the effectiveness of the process.

Shabana Mahmood: Your argument is a very compelling takedown of the political class being a bit rubbish, which we may or may not agree with. You have a point about accountability, but is that not a better argument for improving political accountability in the system, making us work harder in the Commons and making us work harder as an opposition, rather than saying politicians are rubbish, so let us just hand it over to the judges, who apply a whole different set of principles?

Baroness Jones of Moulsecoomb: I am not saying that politicians are rubbish. I am saying that they are only as good as the information they are given. Quite honestly, having watched the Met over the past 16 years, I know that they can be extremely selective about the information that they give you. That may not be true for the security services; I do not know, but I think it likely is.

Shabana Mahmood: If we accept rubbish information, we are failing to do our political job. I still have not heard an argument that says that we should move away from the realm of political accountability to legal accountability.

Baroness Jones of Moulsecoomb: We do not know it is rubbish.

David Davis: That is to misrepresent the argument. The second legal issue here is that I think you will find that for most of these warrants they are forbidden to tell anybody, even the House of Commons. Again, go back and look. I have not read that piece of the Bill—the 299 pages. I cannot remember what it said on it anyway, but most of the time these warrants are incapable of being put in the public domain. You have a problem there too.

Accountability does not work at this level, and you have to ask yourself at the end of the day what you are trying to do. You are trying to have a counterterrorism policy that works and is very effective against terrorism, and works as well as you can make it in relation to the protection of privacy. Those are the two things. We are trying to find an optimum in that. Nobody says that either side has an absolute, I hope, but we are trying to find an optimum in that. The optimum seems to me to be much better with a fully trained judge, with lots of time, with a full case, at any time of night or day, because you will have a panel of them, possibly with a special advocate to argue the counter case. That is guaranteed to make a better decision than a Minister.

Q183 Lord Strasburger: I have to say that the Bishop and I are the only people here on the panel who are not politicians. Some people have suggested that a way out of this conundrum is to keep the Secretary of State involvement in cases of national security and leave it to the judges for the rest. Would that open it up for you?

David Davis: The ISC set one level. I think it was just taking crime out of it. RUSI set it a bit higher, at national security; and Anderson set it a little higher still, effectively at defence and foreign. Anderson had a good argument when it came down to what I think of as the Angela Merkel conundrum. If you are going to bug a foreign Head of State, and I am sure we do not do that, there are political consequences. There are diplomatic consequences to almost any foreign operation. I would have a rather different approach. In fact, the approach in the Bill is okay for foreign operations, so I would draw it somewhere there. I have forgotten who said it now, forgive my poor memory—too much German wine—but somebody said, "foreign and significant people in the UK". I do not accept that one. I think that would be a very bad idea, because you would get back into all the establishment stuff. Broadly speaking, I can see a very strong argument for foreign, but outside that, no.

Lord Strasburger: What about national security?

David Davis: National security is such a hard thing to define. If you are talking about terrorism, whatever the Prime Minister says we are no longer talking about an existential threat. This is not the Soviets or the Nazis. In those circumstances, you could see some sort of argument for clearly defined national security. National security is a very broad-based thing now, with a very small number of targets. I would be inclined to say that you would have to have a narrower definition of that for me to be sure.

Baroness Jones of Moulsecoomb: Perhaps I could note two problems with that concept. The first is that definitions are not defined clearly enough, whether we are talking about national security, operational purpose or whatever. The definitions are, at times, quite slack. The second thing is that intelligence is likely to be shared. There is no limit on sharing information with our allies, for example with the Five Eyes. That is a big problem. It is all very well to accumulate information on what we see as our own national security, but will it impact on others?

The Chairman: We move now to the non-political Bishop of Chester.

Q184 Bishop of Chester: I have been thinking that if we had had Owen Paterson and David Blunkett with the two of you, we would have needed a week for the meeting. Owen Paterson

gave an impassioned defence of accountability at the Dispatch Box as being the appropriate accountability in a democracy.

David Davis: Did he give an example?

Bishop of Chester: When we had Lord Judge, any suggestion to him that the judge would not be entirely independent and able to stand up to all comers was regarded as an offensive suggestion, not least from someone like me.

David Davis: Judges are all saints.

Bishop of Chester: This was what Lord Judge said. Given the architecture as we have it, how can we improve and turn the latchkey into a double lock, as it were? The judges are appointed by the Prime Minister, not the Judicial Appointments Commissioner. They are reappointed every three years. Is there a way of taking the architecture, flawed though it may be, and strengthening it, making the judicial thing stronger and more independent?

David Davis: You cannot make it the best in the world. You cannot make it world-leading, which is what is claimed for this. Mind you, Malcolm Rifkind claimed that the last system was world-leading too, so you cannot make it that. If you want to improve at the edges, then certainly have a judicial appointments panel appoint the relevant judges. It is a technical decision, not a political one. Certainly have longer tenures or maybe even single tenures. Judges I know are inhumanly strong, but they may unconsciously be affected by that.

One of the things in the Bill that I thought was a very bad idea was that in effect it looked as though the Home Secretary judge made a decision on the funding, and it should not be done that way. There should be a Barnett formula for security, where the fraction goes: if you increase the size of the intelligence budget or the secret budget, you give 0.1% or whatever it might be. Make it a formula. Alternatively, you should have a direct negotiation between the lead judge and the Treasury. You must not have the person being checked up on deciding on the funding. Lord Butler would recognise an NAO model, basically.

Q185 Matt Warman: Do you think that this Bill adequately enshrines the Wilson doctrine in statute?

David Davis: Lord Wilson died a long time ago and so did this policy, I think. The Wilson doctrine has always been a very tenuous policy. It is always down to, "If I do this, I will tell the House when I think it is appropriate". That is almost certainly not soon in most cases, by which time the individual Prime Minister has moved on. I would be amazed, to be frank with you, somewhat shocked even, if in the classifications no Member of Parliament had ever been intercepted. I can think of some good reasons over the decades, so I do not think it is quite what it is seen to be in the public domain. It is not a ban on intercepting MPs at all.

In fact, I would take this away from the Prime Minister altogether. I can see even less reason for a politician to judge on whether or not you should tap a politician's phone. If you think of the arguments we have had in the last few weeks, Jeremy Corbyn has been called a threat to national security. Now, I guess it was just hyperbole. Nevertheless, it introduces a question as to who should do this, so it seems to me there are different criteria—and by

the way, they are different from what is written in the Bill, too. The Bill says "MPs and their constituents". In a way, the MPs-to-constituents link is almost the least worrisome, because it is the least interesting to the agencies. MPs to whistleblowers, MPs to journalists, in fact MPs to anybody is what I would make that, and I would make that criterion high.

It is not just MPs, mind you; this is a general privileges issue. With journalists, of course, the Government jumped in and fixed straightaway. You can guess why. The group you are looking at is lawyers, MPs, doctors, clerics and journalists, and none of them should be completely immune. I say that, but again, Chairman, you may remember that at one point some of the terrorist groups in Northern Ireland used doctor's surgeries' receptionists as handoff points, so you cannot make anybody immune, but you have to have a significantly higher threshold, and it really has to be a judge who decides. That is how I would deal with it.

Baroness Jones of Moulsecoomb: I have asked the Met about this and they call us privileged people, those people who come into this group of having certain rights, duties and so on. They apparently do not have a list of us. Obviously that list would change all the time in any case, but they do not have a list, so it is down to the authorising person checking whether or not this person might be a privileged person and whether or not the Prime Minister should be told about the warrant. It is all very specious, I would say.

David Davis: Chairman, I have forgotten one point. One of the things that has become apparent in the last couple of years—it has always been true but has just become apparent—is that communications data is not subject to the Wilson doctrine. Now, communications data is much more important now than intercept, particularly if you are talking about whistleblowers. We have just changed the law in the last year or two, Chairman, to make MPs prescribed people, from the point of view of whistleblowers, and provide them with employment protection. If a whistleblower comes to an MP, he or she gets protection. This is important.

In the Damian Green case, you may remember that Damian Green's arrest was after a whistleblower in the Home Office was in contact with him. That is precisely the sort of thing you have to protect, so the Wilson doctrine has to apply not simply to intercept but to all categories covered in this Bill.

Matt Warman: As I understand it, you are suggesting that these privileged positions should, in particular, be solely a judge, rather than having two politicians, as is currently proposed in the Bill, rather than one.

David Davis: Yes, I would do that.

Baroness Jones of Moulsecoomb: Yes.

Matt Warman: You have said that you would extend that to journalists. Would you care to have a stab at defining a journalist in the modern age?

David Davis: No, I would not. I will leave that to parliamentary draftsmen. The most important group for me is lawyers. Let me tell the Committee why, because this is another of these areas where the Government have the threat back to front. The simple truth is

that when you were in the Cabinet, Chairman, the rule was that if a criminal was being intercepted and started talking to his lawyer, the tape was switched off and the intercept was ceased at that point. That was the rule, as it was understood by the Home Secretary in your day. That is no longer true. The IPT's inquiry into this metamorphosed into the data being recorded but kept in a flagged privileged way, and not shown to the prosecution counsel in any case. Now that is not true and the data is made available to the prosecution counsel.

Now, at some time or another, when one of these comes out, we are going to have a hardened terrorist released on to the streets because of the failure of equality of arms in British law. This is madness. How that metamorphosis happened, I do not know, but it has happened broadly in the last decade or two and it seems to me that we really have to fix that. This Bill has to fix that.

Baroness Jones of Moulsecoomb: This area is so incredibly complex. Lord Chairman, you asked at the very beginning if this Bill is even suitable. I would argue that circumstances have almost moved beyond the Bill at this stage. I took the liberty of sending some of you an encrypted email yesterday and, quite honestly, any criminal or any terrorist could do exactly the same. This Bill will not deal with that sort of thing.

The Chairman: That was a fascinating and a lively debate.

David Davis: It was better than the Berlin Christmas market.

Baroness Jones of Moulsecoomb: I am not sure if it is better than a Christmas party.

David Davis: Chairman, if there are a few issues you have not covered—and I know we are tight on time—can I write to you?

The Chairman: Of course. That applies to both you and Lady Jones. If there are things you would want to add to what you have told us this afternoon, you would be very welcome to do that.

David Davis: It has been a real pleasure, thank you.

The Chairman: Thank you very much indeed. We are grateful.

Lord Judge, Chief Surveillance Commissioner (QQ 47-60)

Evidence heard in public Questions 47-60

Oral Evidence

Taken before the Joint Committee

on Wednesday 2 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Stuart C McDonald MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Bishop of Chester, Lord Hart of Chilton, Lord Henley, Lord Strasburger.

Witness: **Lord Judge**, Chief Surveillance Commissioner, gave evidence.

Q47 The Chairman: Lord Judge, Sir Stanley and your staff, thank you very much indeed for coming along to us this afternoon. As you know, this is a very important Bill. The Prime Minister described it as the most important of this Session. Much of the Bill refers to the change in oversight provision, so we are very grateful for your coming along. I wonder whether you want to say anything yourselves before we start asking some questions.

Lord Judge: I would like to say something, particularly in view of the discussion that has been going on with Sir Mark. I cannot think that anyone would have designed the present three-bodied system. It would never have happened; it should not have done. We work piecemeal on the legislation; we produce piecemeal results; and we have produced three bodies, all of which have responsibilities in the broad sense that we are talking about and all of which work in different ways.

Let me give you some "for instances". Sir Mark has just given evidence to you. He is the commissioner. He has no inspectors. Sir Stanley will tell you that he is the commissioner and, with his team, he has 10 inspectors. I will tell you that I have taken over the surveillance commission. I have seven inspectors, who are former police officers of no less than superintendent level, a Chief Surveillance Inspector, six commissioners, three assistant surveillance commissioners and, good heavens, there is even me. We all operate differently. The focus so far has been on Sir Mark, and I know that IOCCO, as it is called, has had quite a lot of input, but can I just explain to you how this leads to confusion and can be improved?

The Chairman: Please do.

Lord Judge: We have had to take on oversight and prior approval of undercover police authorisations. We all know about the relatively recent disasters caused by officers going wrong in undercover operations. There is an application to us and, mark this: we have to authorise. Neither of the other two Commissions authorises. Every single piece of intrusive surveillance, certain types of property interference and long term undercover operatives

for which we are responsible is authorised in advance by a commissioner, who is a former judge.

The case is made out to us that there should be an undercover police officer in this particular, rather serious drugs case. The authorisation is made. In goes this brave young man or woman—and most of them are very brave young men and women—and they discover that there is quite a lot going on and it would be a good idea to have some intrusive surveillance, say into a car that is being used to transport the proceeds of drugs. He has to go back to his authorising officer. The authorising officer comes to us, and there is another application for intrusive surveillance to take place. That takes place, and that reveals something else: these drugs are actually to do with a potential terrorist ring.

That does not come to us; that goes to Sir Mark, but there is no pre-authorisation by him. Somebody says, "We had better have some communications input". That goes to Sir Stanley. There is no pre-authorisation by him. Now, I am sorry to say this, but telling the story the way I have is entirely accurate. If you thought about it, you would say, "Is this really the way we are doing business?".

Speaking only for my own team, every authorisation is made before any of the aforementioned intrusion takes place. The papers come to us, and I have a complaint about the quality of our equipment, but that is another question. A judge commissioner looks at them. He decides whether necessity is established and whether it is proportionate, which involves looking at the nature of the offence. You would not authorise intrusive surveillance for somebody who was stealing a tin of salmon from a supermarket. You are looking at sentences starting in the three to four-year range and upwards. He checks for proportionality: is this a reasonable way to go about sorting this problem out? He authorises or does not, or says, "I want more information". Then the process goes through.

At the other end of the process, every year my inspectors go in and conduct an inspection of every single police force in the country, Her Majesty's Revenue & Customs and so on—all the law enforcement bodies. They conduct random analyses inspections of all the things for which the body is responsible, such as encryption. There are all sorts of different things that come under the remit of covert surveillance. They then write a report. The report is written to me. It goes to the chief constable. I write my own report to the chief constable. Sometimes I say, "This is being very well handled. Your authorising officers are well trained. The paperwork is very good. The explanations are excellent", and so on and so forth. I have just written a very rude letter saying, "This is not good enough. You are not complying. There are too many breaches. There is too much inefficiency in this part or that part", or whatever it is.

I write that to the Chief Constable, and then I go and see him, or one of my commissioners does. I go to all the big Forces. We discuss the report for the year. Most of the time—and this I hope does not surprise you—the chief constables are as anxious as we are that the job should be done properly. Apart from the reputational matter, they are men, and women now, who want the job done lawfully. They are also aware of the dangers of evidence being excluded at the trial process or an abuse of process argument leading to the whole prosecution being discontinued. I go there; we discuss it. If I am unhappy, I will go again. I have not had to, but I have only been in this job for a relatively short time.

I am not recommending it to you, but our system is very different from the one you have been discussing with Sir Mark, and from Sir Stanley's. The idea that we should have a surveillance system in which there are three different bodies is itself absurd, and then three different bodies operating differently strikes me as daft. That is my opening statement.

The Chairman: Very interesting it was, too. Sir Stanley, do you want to make any comments?

Sir Stanley Burnton: As you know, I am the new boy on the block. I have the good fortune to have staff who have received a glowing report from David Anderson, as you will have seen. They have a range of competencies, including computer abilities. There were questions asked of Sir Mark about training. I have some computer knowledge; I was judge in charge of IT, but I could not go into a public authority and interrogate their computer system. We have inspectors who can and do just that.

We carry out an audit function. I believe that you cannot carry out an audit function properly unless you have some understanding of the business you are auditing. That does not mean to say you could do it yourself. I could not go into a computer and interrogate it to see how many search or interception warrants had been issued, and view the grounds and so on. But I like to think I have a sufficient understanding of what staff can do, and do, to carry out the functions of my office.

Like Sir Mark, as far as I am aware, there was no special security clearance carried out when I was appointed. On the other hand, when I was a judge, I used to do Special Immigration Appeals Commission, or SIAC, cases, which concerned terrorism and people who were alleged to be terrorists, so I have some acquaintance with that part of the job. Of course, I did criminal work, so I have some acquaintance with that area as well.

Q48 **Lord Butler of Brockwell:** May we take it from Lord Judge's and Sir Stanley's opening statements that you think it is a good idea that this Bill in future sets up a single Investigatory Powers Commissioner?

Lord Judge: I have no doubt about that. We also have to make all the three current bits of the system work in the same way. I personally think, although I have no experience of IOCCO or Sir Mark's work, that the authorisation process is one of the strengths of what we do. You have to have an authorising officer who persuades you that this is appropriate—i.e. necessary and proportionate.

Lord Butler of Brockwell: If I may then clarify my understanding of this, in your area, Lord Judge, there is pre-event judicial authorisation.

Lord Judge: Of every item of intrusion that comes within our jurisdiction for prior approval by a Surveillance Commissioner.

Lord Butler of Brockwell: In Sir Stanley's area, this Bill will set up, except in the most urgent cases, pre-event judicial authorisation. Is that correct?

Jo Cavan: It will in relation to interception warrants, but it will not in relation to acquisition and disclosure of communications data, which is the bulk of our remit. Around 500,000 requests for communications data are made on an annual basis, by a rather large number

of public authorities. The judicial authorisation and the double lock that the Bill introduces are only in relation to the interception warrants, of which there are around 2,700 a year.

Lord Butler of Brockwell: Thank you very much. Then, if I understood what Sir Mark said, in the case, however, of somebody placing a bug in premises, there will be no judicial pre-event authorisation. There will be a warrant, but there will not be a judicial pre-event authorisation.

Lord Judge: If it is an application under part 3 of The Police Act 1997, which we deal with a lot, there will have been a pre-judicial authorisation in advance (for activity in a private vehicle or premises). This is why the system desperately needs to be shaken up.

Lord Butler of Brockwell: What about in the case of the intelligence agencies? Did I misunderstand Sir Mark?

Lord Judge: No, you did not. The intelligence agencies work differently. If it is an ordinary police investigation, yes, every piece of intrusive surveillance is pre-authorised. In the case of intelligence, it works differently.

Lord Butler of Brockwell: In the case of an intelligence agency, at the moment and under the Bill as proposed, there is no pre-event judicial authorisation of the warrant.

Lord Judge: No.

Q49 **Suella Fernandes:** What do you think about the safeguards provided in the new system as compared to the current one? Do you consider that there are better safeguards under the proposed system?

Lord Judge: I think that pre-authorisation is something Parliament needs to look at across the board—but I would, wouldn't I, because I am convinced about our own little bit? If you do that, the papers come through to a commissioner, who knows what the law is, knows what he—or she, but we do not actually have any females—is looking for. If it is not good enough, if it is an urgent or relatively urgent thing, he speaks to the authorising officer, saying, "This is not good enough. Tell me more about this" or, "I am worried about the possibility that this suspect's wife is going to have her life intruded on". If satisfied—and usually you are, because they do not come unless they have a good case—then it is authorised. Then you inspect at the other end and you go through them.

I will add this, which I did not mention when I made my opening statement. From time to time, my inspectors will tell me that they are very worried about the commissioner having given an authorisation. They are not just examining the way the police are doing their work; they are a form of check that the commissioners are applying the law. Of course, it does not happen very often, but that is part of the process and I welcome it. If there is a case where I think the commissioner was wrong to make the authorisation, then I see him and say, "I think this was wrong" or whatever.

Provided that you, as the citizen, are satisfied that, before people can come intruding in your life, a decision has been made by somebody independent of those who are going to do the intrusion, and there is a system for inspecting afterwards, at random, what the various bodies have been doing, that is a pretty good form of safeguard. In my experience—again limited—I do not see cases where people or authorities are applying unless they have good grounds for doing so, because they know they will be refused.

Q50 **Lord Strasburger:** My questions are for Ms Cavan. I would like to start by congratulating you on the transparency of your reports and your engagement with the public through Twitter. I wonder if Mr McDonald's concerns about systemic difficulties and unwarranted activities would be allayed by the new commissioner being able to initiate inquiries on his or her own initiative, and perhaps even unannounced inspections. That is my first question.

Jo Cavan: On that note, we recently published a wish-list of some of the ways we feel the oversight provisions need to be strengthened. In one respect, the ability and mandate of the new commission to launch inquiries or investigations, we feel, could be further strengthened. We also feel that access to technical systems could be more explicit in the clauses. At the moment, the drafting is outdated: it refers to providing the commissioner with information or documents, whereas these days we are generally not looking at paper. When our inspectors go in, they have full access to the technical systems; they run query-based searches and look for compliance issues at scale, which is really important when you are dealing with these bulk collections. We think the oversight provisions and the clauses concerning technical system access and the ability to launch inquiries and investigations could be strengthened further.

Lord Strasburger: Lord Chair, would it be appropriate to invite Ms Cavan to put her views on how that might be strengthened to us in writing?

The Chairman: I am sure that would be fine.

Lord Strasburger: My second question is: how do you think we should strengthen oversight of international co-operation between Five Eyes intelligence agencies?

Jo Cavan: There are some additional safeguards in the IP Bill for the sharing of intelligence with overseas agencies. These matters have been significantly debated during some of the recent Investigatory Powers Tribunal cases. As a result of further disclosures made in those cases by the Government, the safeguards have been published and they are now in an amended code of practice. Certainly, that is an area we are looking at during our inspections and audits.

Sir Stanley Burnton: The fact we can interrogate the computer records of the authority whose activities we are auditing reduces the need for unannounced visits, because we have access to the raw data.

Q51 **Victoria Atkins:** Following on from Lord Judge's very helpful analysis of the oversight and review process, there is one angle that I am not sure the Committee has heard about yet, which is what happens at trial. Where an investigation results in a suspect being charged and a prosecution being brought, could you help us, please, with the duties on the prosecuting lawyer and prosecuting counsel to ensure that any warrants that may have been used during the course of that investigation were conducted properly, and the professional obligations on them as a reviewing process, in addition to all the reviewing processes you have already described?

Lord Judge: When everything has worked as it should have, and there has been no breach and no subsequent concern, that simply goes through. There is no disclosure. But, where there has been any breach—and, as Sir Mark pointed out, there are self-reporting breaches

as well as discovered breaches—it comes to me, and it is axiomatic that the first thing I do, having decided what should happen about the breach, is to say all the papers must now be retained and disclosed to the Crown Prosecution Service, in the event of a prosecution, for onward disclosure as seen fit. That is up to the prosecutor. That material, I am sure, would then go to counsel for the defence, who would then decide whether to make an application or not.

The other feature, which has been underlined by a recent decision in the Divisional Court called Chatwani, is that there is an obligation—it is obvious that there is, but the court has said so—on the person making the application to tell the whole truth. In other words, you set out the points you say are favourable to the application you are making and the authorisation you are seeking, but you also have to add the bits that do not fit. Chatwani was a case where what was going on was not properly disclosed and the Divisional Court said, "Quite obviously, you cannot work on the basis that the whole story is not told". Failure to tell the whole story would itself constitute a breach, which would then have this system fall into place: retain it, keep it, disclose it if there is a prosecution. Of course, often there is not a prosecution, which raises a different problem, but if there is that is how it is done.

Victoria Atkins: In addition to the many sets of eyes in your organisations, there is also, if a case comes to court, the extra review conducted by lawyers and counsel to ensure that processes have been applied properly.

Lord Judge: Yes.

Q52 **Baroness Browning:** You heard me ask Sir Mark about training. I wonder what training you feel might be necessary for the new judicial commissioners.

Lord Judge: Rather like Sir Mark, what you are doing is making a judgment. This is what, if you are a former judge, you have been doing for however many years you have been doing it. You have been making decisions like this day in, day out. The questions are very simple: is this necessary? Where is the evidence? Yes, on this evidence, it is necessary. Is this proportionate? I must bear this in mind and that in mind, and that in mind. On this evidence, that is proportionate. Hang on, there is a bit of this that might involve the suspect having had conversations with his, for the sake of argument, doctor. You have to be careful there. I mentioned earlier an intrusive surveillance into the family car that is being driven by the wife. Nobody suspects her of anything, so you cannot have that; it is not proportionate.

That is all you are doing. You are making a judicial judgment, which is what you have spent your whole career doing. I am not saying you are infallible, and I made the point a few minutes ago in relation to my commissioners: when they get it wrong, my inspectors will tell me. But you do not need special training for that. What happened to me is, in effect, I went and shadowed my predecessor. I went out on inspections to see what my inspectors did and how they went about it, and to see that they were doing the job the way I wanted them to do it. I go out with my commissioners. We meet regularly and discuss the problems that are current. That is the training, and then you take over the job.

Baroness Browning: With the advance of technology and things moving on so quickly, particularly once this is in one collective body, could the choice of methodology in the application that comes before you be something you question—whether this route is going to be used or that route? Does that not require some technical knowledge on the part of the person making the decision?

Lord Judge: Not really, because, for necessity, that does not arise. You do not need to know whether the nature of the intrusion is a probe that is one inch long or six inches long; you need to know whether there is going to be a probe. Of course, I have overlooked this. I spent time, two days ago, sitting in the National Crime Agency, being lectured to about how some of the worst aspects of child pornography being transmitted around the world are dealt with. We do try to keep up with that.

But, no, you are making a judgment. In the new system, I have no doubt—and I disagree with Sir Mark here—that there should be one or two people with serious expertise in technology. I also think there should be a legal adviser. The law is extremely complex. RIPA is a dreadful piece of legislation. I say that with some strength of feeling, having had to try to understand it. Why do judges need a legal adviser? For that reason: to say it could be any one of 17 possible interpretations, rather than the five you thought you had. More importantly, in this system, from time to time you need advice. That is what I would like to happen, but then I envisage this as rather different from the bits and pieces you are seeing put together before you today.

Q53 **Lord Hart of Chilton:** You heard us discuss with Sir Mark the question of the judicial review principles that underlie the judge's oversight. I wondered if any of you would like to comment further on what he said. We were exploring whether it is right to call it a real double lock system. Are there any points you would make, further to the points made by Sir Mark?

Sir Stanley Burnton: Judicial review is not simply a question of looking at process. In the context we are discussing, the commissioner has to look at necessity and proportionality. The degree to which judicial review is imposed as a test and the stringency of the test depend very much on the context, the facts of the individual case and the consequences of the administrative or governmental decision in question. In the context we are discussing here, it is not unfair to describe the process as a double lock.

Lord Judge: That is rather my view. My only hesitation, which is a lawyerly one but not totally without some force, is in using the words "judicial review" as a description of the test that has to be applied by the judicial officer. Judicial review used to be Wednesbury unreasonable mad. We would call it Wednesbury unreasonable, meaning only an idiot could have reached this decision. Nowadays, judicial review is less stringent than that: "He is not an idiot, but it is a really stupid decision". That is not quite the same. "I am not sure many people would have reached this decision" is another test. We need to be slightly careful.

If you are talking about the Home Secretary, and I think you are, I have a separate point. There is a difference between national security warrants and ordinary criminal warrants. What we do should be the system for ordinary criminal warrants: an authorisation in advance. That is a double lock. National security is rather different. The Home Secretary has the most amazing responsibilities in relation to that. Judges second-guessing is simply

inappropriate. You have to have a stringent judicial review test. I am now coming back to what Sir Stanley said. You know you are dealing with national security; you know somebody might be planting a bomb. You are going to be very cautious about interfering and saying, "This man or woman, who is the Secretary of State, is daft". So I think the double lock system will work pretty well.

Sir Stanley Burnton: You can forget about Wednesbury unreasonableness in this context. Interestingly, proportionality and necessity are tests that we have imported from Europe, and the proponents of the Bill are clearly happy to adopt them in this context.

Q54 **Matt Warman:** As a still fairly new Member of Parliament, it struck me, observing the procedures of Parliament, that, if you have some pretty crazy procedures around for long enough, they become lauded as institutions. You described a pretty crazy set-up in your opening remarks, but does it not function as a sort of quadruple lock on what we have already, if you are constantly going back to ask for re-authorisation? I wonder what we are going to lose by streamlining it, if anything.

Lord Judge: I am sorry, I must have been unclear. They are not re-authorisations. Each one is a fresh authorisation by a different body. Sometimes the body will not even know what the earlier authorisation was. It is not a quadruple lock at all. Each is an individual one.

Matt Warman: So you do not see any strength from having three different people.

Lord Judge: No. I see potential for confusion. A much more coherent system would enable the same commissioner to look at one case. "This is the case of Snooks. This is the drugs ring. Right, the undercover officer has gone in. Here he wants this. Does the authorising officer think this is appropriate? Yes", and so on. The whole thing can be kept, in effect, under one person's eyes. It is much more proportionate. Sorry I was not clear enough. They are separate organisations.

Matt Warman: The argument that has been put is: at the moment, we have three commissioners, and, if one person makes a mistake, who is checking up? You would not accept any of that.

Lord Judge: People make mistakes, certainly, but we are all independent organisations. We talk; we discuss problems together, but we operate completely differently. It is not a system with the three sections of this keeping an eye on each other. We do not.

Q55 **Lord Butler of Brockwell:** When we took evidence from Home Office witnesses last week, they introduced a new concept, new to me anyway, of rationality. We asked whether reasonableness would be a test, and the witness seemed to dissent rather. He made a distinction between rationality and reasonableness. Is that a distinction you recognise?

Sir Stanley Burnton: The Wednesbury test is a rationality test: that no sensible administrator or executive correctly applying the law could have reached this decision. It is not a very stringent test; it is only in extreme cases that you are able to say something is Wednesbury unreasonable, whereas proportionality and necessity are more stringent.

Lord Butler of Brockwell: You are saying that there is no great distinction between reasonableness and rationality.

Sir Stanley Burnton: I am.

Lord Judge: I would not have noted any difference between them. I would not have argued the point with you. If you had said "Is it reasonable?", I would not have said, "It has to be rational".

Q56 **Stuart C McDonald:** I have a rather more mundane question about money, I am afraid. The impact assessment suggests that the new oversight and authorisation regime should cost around £150 million over 10 years. Would you regard that as realistic? If you do not feel able to answer that particular question, would you say that you have had sufficient resources to carry out your jobs fully, or are there other things you would have liked to do that you have been constrained in?

Lord Judge: I could give you a list of my complaints.

Stuart C McDonald: Please do.

Lord Judge: Our technology is, for obvious reasons, supposed to be secure. Our Brexit system—I am so sorry; I have something else on my mind—our BRENT system is hopeless, so we want it improved. We wait too long for new appointments to happen, and so on and so forth. Parliament has to decide how much it is going to spend on protecting the citizen from the threats of crime and terrorism, and how much it is going to spend on ensuring that those who should not be being surveyed in any way at all are protected from it. If you go down this route, you will have to have—I would strongly recommend if I were asked, so I will tell you anyway—a location separate from the Home Office, and people working there who are not drifting in and out of the Home Office. The perception of independence is strengthened by going to a separate place.

I mean no discourtesy; our rooms are pretty cramped. You are going to have a big system. If you have the same number of commissioners I have, which is six plus me plus three assistant commissioners, that is ten before you start. If Parliament enacts a system in which there is authorisation for everything in advance, it is going to take a lot more people. It will cost a lot more. We can either do it on the cheap or spend more money. We are in times of great financial stringency. I am sorry, but this is really not for me to say. I might say it in a different role, but not here. Yes, it will cost a lot more.

Sir Stanley Burnton: I am not an accountant and I cannot give you a figure. My impression is that in order properly to run the system, there are going to be something like eight judicial commissioners, which is quite a lot of staff. They must be backed up with appropriate staff, with the kind of skills my office now has but more widely available. There will be more inspectors, who must be appropriately qualified. You are looking at significant sums of money.

Incidentally, on a question that Sir Mark was asked, it ought to be the chief commissioner who determines what staffing and resources are needed. He must, of course, approach the Treasury and agree a budget, but it seems to me to be inappropriate for the person who is being monitored in a sense to be the person who decides on the resourcing of the office. Indeed, internationally, one increasingly finds that judicial bodies are not subject to a

Ministry of Justice, so far as resourcing is concerned. It is the judiciary that determines the resources it requires, subject to Treasury agreement.

Lord Judge: I entirely agree with that. The idea that judges will be looking at the Home Secretary's decisions and saying, "We do not think that is right", and then going cap in hand to that same Minister is not a sufficient separation.

Stuart C McDonald: That is helpful, thank you.

Q57 **Lord Henley:** I asked Sir Mark earlier about cost. This takes me on from Stuart's questions. Are you saying that under the new arrangements you should, almost as the universities used to in the past, negotiate directly with the Treasury without any intermediary?

Lord Judge: That would be my view. I make this clear: I am not seeking appointment to be the high panjandrum for this. A direct communication between the Treasury and the Commissioner is the way to do it.

Sir Stanley Burnton: As a matter of principle.

Lord Henley: Is that because your independence would be undermined if you had to go through the Secretary of State?

Sir Stanley Burnton: The appearance of independence is undermined if one has to go through the Minister whose work one is supervising.

Lord Henley: I ask that purely because I remember, back in the long, distant past, that that is how university funding used to be done when universities were independent. It is no longer the case; there is a department that looks after universities. That might be the way forward.

Lord Judge: In the context of the way the judiciary works, there has been coming and going about this, but I used to agree a budget or not agree a budget. I also had the power, which I never exercised, not only to write and say, "I do not agree it", but to say, "I am going public and this will not do". You need some kind of arrangement like that. We are both in the same place. If we are going to supervise the Home Secretary, we must not be answerable to him or her for the money.

Q58 **Lord Strasburger:** Would you be attracted to the system that exists in New Zealand, where the people in your position have a fixed percentage of the spend on intelligence and policing, and the decision is taken out of politicians' hands?

Lord Judge: The decision as to money?

Lord Strasburger: Yes.

Lord Judge: Ultimately, the Government have to find the money, so there has to be a discussion with somebody who represents the Government. Therefore, that is why we both say the Treasury.

Sir Stanley Burnton: I think I would need notice of that question.

Jo Cavan: If we went to that type of model, our percentage would no doubt be significantly lower than the percentage in New Zealand, because of the larger scale of our intelligence agencies, in particular the bulk collection we do, in comparison to New Zealand. Anyway, I do not necessarily think it is a bad model. I would say that the legal mandate and oversight provisions the New Zealand inspector general has are far more explicit and comprehensive than the ones in this Bill.

One of our points on the clauses around oversight is that they relate only to judicial commissioners; they do not relate to the commission. If we are going to create this world-leading oversight commission, it is important that the commission is explicitly referenced and the legal mandate, powers and functions are comprehensively covered.

Lord Strasburger: For the second time, I will say something about judicial review. I asked the Home Office on Monday why the words "judicial review" were in there, and they could not really tell us. What would be the effect, do you think, if they were struck out? Would the Bill be better for it, or worse?

Lord Judge: Parliament has to decide what function the judge is to exercise. Judicial review is a well-known series of principles, even though occasionally you hear it expressed in different ways. As I said a few minutes ago, in terms of national security, the idea of the judge in effect making the decision simply cannot arise. If a bomb goes off in London tonight, it will be the Home Secretary who will be down there. It will be she who has to answer to the House about what has gone on; it will not be the judge. We have to be careful to remember that there is a political responsibility, which is in the hands of the Minister, and we cannot dilute that.

Sir Stanley Burnton: If I remember rightly, the legislation on control orders, which are orders short of imprisonment to control people who are suspected to be terrorists, also requires the judge to apply a judicial review test. In practice, of course, in SIAC, the judge hears, often in secret, the evidence that is available to show that someone is a security threat. He applies quite a stringent test, because he has the information and knows whether there is something justifying imposing a control order. The legislation has changed, but it is not dissimilar.

Q59 **Bishop of Chester:** The fear in some quarters is that this new system will end up with rubber-stamping, that it will not be sufficiently independent. That is the fear abroad in some quarters. I am trying to imagine life in the increasing digital swirl in the years to come, with the exponential growth in communications and means of communication. How can we get some feeling of control and exercise oversight, and not simply be carried along in the tide? The threats in the 21st century will probably increase as well. Can you give us some idea as to how this double lock, this independent supervision, will work in practice?

Lord Judge: I hope I am not being discourteous. It is very easy to drum up anxieties. I am just as worried about criminals being able to get hold of information as I am about any of the authorities. We concentrate on the authorities. I do not know what is going on in this room even as we speak, but the technology available to serious criminals is, at the very least, as good as is available to law enforcement people. You trust your judiciary to make decisions against the state when it is appropriate to do so. I do not think anybody suggests that the judiciary nowadays is less independent than it was. In many ways, it is more so.

You have men and women who have exercised these functions all their professional lives, first at the bar or as solicitors, then as judges. They are men and women of proven experience and quality. You just have to work on the basis that you should trust them.

Bishop of Chester: Would it be better for perception, if nothing else, if the appointment of the commissioners was not made by the Executive. Just as you made those comments earlier about having clear blue water between the Home Office and this, would it be better to involve an agency more independent than the Executive?

Lord Judge: It is the Prime Minister's appointment. The Queen appoints the Lord Chief Justice, but that is on the recommendation of the Prime Minister. I do not suppose the Prime Minister spends a lot of time deciding what he is going to recommend to Her Majesty. There is, in the case of the judges, a Judicial Appointments Commission. I would not recommend that for these appointments. Apart from anything else, they have far too much to do and it takes a very long time.

For the very last commissioner who was appointed to my team—and this you could consider—a senior serving judge and a member of the Judicial Appointments Commission sat together, with my predecessor as an observer, and they chose whom it should be, and the appointment was then made. That is a perfectly sensible system. It is only theoretical that the Prime Minister has anything to do with it. It is very nice for me to be appointed by the Prime Minister, but I honestly do not suppose anything more.

Sir Stanley Burnton: By prescription, the commissioners are going to be either actual serving judges or former judges, and so one has to bear in mind that they will have been independently appointed, initially. Whether they will be full-time judges working part time as commissioners or are expected to be full-time High Court judges seconded to the commission, the Bill does not make clear. We probably both have concerns about the ability of the existing High Court to have people seconded to a different function, given that the High Court itself is under pressure.

Jo Cavan: Before we move on, I wanted to talk about the end-to-end process, because a lot of the debate has been focused purely on the double lock and the authorisation process in the first instance. Yes, that is crucial, but what is equally crucial is the post-facto audit functions, which look at the process from end to end. We carry out over 200 inspections a year and make over 800 recommendations to improve systems and procedures in compliance.

The inspectors, during their inspections, are looking at post-authorisation: was the actual intrusion foreseen at the time the warrant or authorisation was given?; has the conduct become disproportionate because the level of intrusion was not anticipated? They are looking at how the material that has been gathered has been used. Has it been used in accordance with the purpose that was set out in the warrant? They are looking at the retention, storage and destruction procedures for that material. They are looking at whether any errors or breaches occurred as a result of the conduct. All those post-authorisation functions are critical to ensure that you are overseeing and auditing the end-to-end process. That is where the modification and ongoing review of these provisions come in.

Sir Stanley Burnton: The reviewer will also look at the duration of the warrant and may go to the public authority concerned and say, "How is it that this warrant has been renewed twice? What evidence have you been gaining from it? Was there any justification for its continuation for such a long period?'

Q60 **Mr David Hanson:** In relation to Clause 176, which establishes the budget, as we have discussed previously, are you therefore suggesting to the Committee that we should consider recommending a rewrite of that clause that separates completely the funding from the Secretary of State, not just in terms of the effective micromanagement that the clause could imply, although in practice it probably will not, but in terms of the principle that the Treasury should be the lead department that you directly negotiate with?

Lord Judge: If we retain the present Bill in relation to judicial oversight of the Home Secretary, yes, unequivocally.

Mr David Hanson: I have a second point. Lord Judge, I noticed you made the point that it is very nice to be appointed by the Prime Minister, but you are sure he does not take much interest in it. I suspect, as many people in the past, should you be a troublesome priest, he may take some interest in your reappointment. I am wondering, given what the Lord Bishop has said, whether or not consideration should be given to independent appointment, rather than direct ministerial appointment, into the oversight role, given that oversight role?

Lord Judge: If we envisage that, 20 years from now, the Prime Minister of the day decided that he or she was not going to re-appoint somebody, and had no good grounds for doing so save that he or she did not like the colour of their face, or whatever it might be, there would be an absolute scandal. I really do not think Prime Ministers would want to get embroiled in that sort of thing.

We have to be careful about public perception, if you do not mind me saying so. Most members of the public, I suspect, want to know that those of us who have responsibilities in this field are seeing that the job is done efficiently, ie to protect them, and fairly, to protect their own rights. That is what they want. I do not think that they are going to be terribly fussed, largely, about whether the Prime Minister's name goes on the appointment, or whether it is that of the Speaker of the House of Commons or the Lord Speaker. One has to be careful. That is my view about it. If I were in charge and, the Prime Minister failed to re-appoint somebody and I thought this was the reason, I would go and see the Prime Minister and tell him, "I will go public about this".

The Chairman: Thank you very much indeed. It was a fascinating session and we are grateful to all of you for coming along. You have given us very interesting stuff to chew over, to say the very least. Thank you very much indeed.

Lord Judge: Thank you.

Eric King, Visiting Lecturer at Queen Mary, University of London (QQ 207-215)

Evidence heard in public Questions 207-215

Oral Evidence

Taken before the Joint Committee

on Monday 21 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Suella Fernandes MP, David Hanson MP, Shabana Mahmood MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Lord Hart of Chilton, and Lord Strasburger.

Witness: **Eric King**, Visiting Lecturer at Queen Mary, University of London, gave evidence.

Q207 **The Chairman**: A very warm welcome to all three of you. Particularly as we are so close to Christmas, it is very good of you to come along and give us the benefits of what I know is your considerable expertise, knowledge and experience. We very much look forward to listening to you. I will start by asking you a general question, which will give you the opportunity, if you so wish, to make any general statements about the Bill. Will it work? What are your views on the draft Bill from a technical standpoint and are these proposed powers workable? Perhaps we will start with Professor Buchanan.

Professor Bill Buchanan: Thank you. I would say that we live in a very different world from the one that we did. We have built this cyberage within about 40 years, but the infrastructure that we have created is very fragile. We must protect citizens from hackers and so on. We must protect privacy and identity. More and more services are moving towards the provision of both privacy and identity. Individuals need to be assured that they are not being spied on by cybercriminals across the world. They also need to be able to prove their own identity and the identity of what they are connecting to.

Encryption involves both these aspects. It keeps things private but it increasingly is also used for identity provision. Much of cryptography is now focused on proving the identity of the services that we connect to. Just now, most of the services that we use in the cloud—Google, Amazon, Facebook and so on—are encrypted. Every time we see "https" and we see a green bar on our browser, it means that we are protected with a unique cryptography key for every session that we create. It is almost impossible to crack that key without knowing the private key of the site to which we are connected. The only way that someone could crack communications through a tunnel such as that is to get the private key off the company that is involved in the communications, which would involve Microsoft, Facebook, Twitter and so on handing over their private keys. The problem around that is that if someone gets access to those private keys—those special keys—we open up the whole of the internet and we will have the largest data breach that has ever been caused.

The communications that we have are obviously highly sensitive. The logs that we see on the internet are really the history of our whole lives. They are our thoughts, beliefs and dreams almost by the second. Every single thing that we do is recorded in our web history.

The amount of money that that would be worth to a criminal—a cyberhacker on the internet—would be almost unlimited. If an ISP was hacked, you can imagine what the logs could be used for and what bribery there could be for individuals and companies. A balance needs to be struck between the privacy of individuals, the protection of our businesses and the risk of serious organised crime.

Erka Koivunen: Lord Chairman, it is an honour to be present in this Committee session. It has been a fascinating journey to read through the Bill, in particular as a non-native speaker—it has been a tedious task. However, I would like to offer my congratulations. The Bill is pretty transparent in the way in which it lays out the intentions of the Government to do a lot in terms of law enforcement and signals intelligence. This is a Bill that you would get if you asked signals intelligence organisations what they would like as a Christmas present; they would reply that they wanted this and wanted it in bulk.

However, there are some unintended consequences when writing broad legislation that would give such exceptional powers to intelligence agencies and law enforcement. If there ever was a question whether nation states, Governments and military organisations would be engaging in hacking and computer intrusions, I guess that this Bill solidly sates that, yes, this is what they do and this is what the UK Government are actively seeking to do. Frankly, this is something that has been going on for quite a while now. The Bill is an attempt to put the existing situation in writing. We, as a provider of cybersecurity services to private companies and Governments, would typically advise our customers to be aware of criminal activity taking place and of their organisations being targeted by nation states and Governments as well. No better marketing material for services such as those that we provide could be envisaged. We should be aware that the powers laid out in the Bill could be misused. This will lead other nation states to try to mimic these powers. As a member of the European Union—I come from Finland, I am a Finnish national and our company comes from Finland—I feel that I am now a target of many of the activities laid out in the Bill. I do not think that this is what I signed up to when I joined up the cybersecurity profession. There are lots of discussions on how to limit those powers. I am not a lawyer or a legal person, but there are lots of things I can imagine technically that would undermine our society's security. Some of the things that we build in our online systems depend on strong cryptography, in terms of encryption, authentication and authenticity.

The Chairman: Thank you so much indeed. It is very good in English and in Finnish. Mr King?

Eric King: I will not repeat any of the feelings and concerns that both Bill and Erka have highlighted, but perhaps I can help the Committee in one regard by focusing your minds not on the question of whether the proposed powers are necessarily workable, because the majority of them are in fact already in use. That is not to say that they are powers granted by Parliament—indeed, I would expressly say that that is not the case—but they are powers that our agencies have been deploying for a number of years.

It has only been this year for the most part that the public have found out about these and that they have been officially avowed. It was in February this year that the Government avowed hacking for the first time—it is now called "equipment interference". In the Investigatory Powers Tribunal a few weeks ago, I heard from government lawyers that bulk equipment interference apparently had still not been avowed. Bulk interception was only avowed with the writing of the ISC's report in March this year, for which we are very

grateful. The use of bulk personal data sets, as mentioned in the Bill, were again revealed to the public only with the ISC's report in March. The ISC stated at the time: "Until the publication of this Report, the capability was not publicly acknowledged, and there had been no public or Parliamentary consideration". Bulk communications data acquisition was only avowed on the very day that this Bill was introduced to Parliament by the Home Secretary, who admitted that our Security Service, MI5, had been acquiring in bulk the phone records of everyone in the United Kingdom. Anderson commented at the time to the BBC that the legal power that had been relied on to exercise that authority was so broad and the information surrounding it so slight that nobody knew that it was happening.

I make these points to say that the Government, in my mind, should make operational cases from first principles for every single one of these powers. Simply because they have already been in use and simply because the agencies have interpreted law in a manner that they feel has made them lawful does not make them lawful. It is right that Parliament should receive a full operational case for each and every one of these powers. It is a matter of assessing not whether they are merely helpful or offer some form of value, but whether, given the scope of everyone's lives that they touch—after all, that is what bulk powers do—they can be vetted and scrutinised to make sure that they are both necessary and proportionate.

The Chairman: Thank you all three very much indeed.

Q208 **Shabana Mahmood:** I want to ask you about future-proofing the Bill. When the police, Home Office and others gave evidence to us, they were pretty robust in their view that these powers were sufficiently future-proofed against behavioural and technological change, as the powers were broad and wide-ranging. Other experts, in evidence, scoffed at the very idea of future-proofing, because of the pace of change in technology and how that impacts on behaviour in the online and digital space. What are your views on whether future-proofing is possible and, if so, whether that has been achieved in the draft Bill?

Professor Bill Buchanan: If there is one change that is happening in systems just now, it is a move towards the cloud. So like it or not, most of our emails are stored in the cloud, possibly in other jurisdictions. The main moves are with tunnelled web access. If someone uses a tunnelled connection, you cannot see the detail of the information that is passed. The minute someone uses https there is no way that you can see what page they accessed on the site; you can see the IP address but you cannot see what they clicked on. The whole world is moving towards https. Google is almost forcing companies to sign with a digital certificate or they will not be ranked highly. Many companies are moving towards adding a digital certificate. There is now a service online for free; you do not have to pay for a certificate any more. So increasingly companies will be signing their sites. Once they do that, communications are likely to be https.

There may come a time when many service providers will accept only secure communication. It is likely that our old protocols—http, Telnet, SMTP—will be switched off and replaced by the s version, the secure version. More and more people are using VPN connections. If you are a businessperson you will use a VPN connection if you are on the road. VPNs cannot really be cracked at all. Along with that, more people are using proxy systems where the accesses are not coming from their own computer but from another computer. Increasingly we are using public wi-fi to access the internet. It is extremely

difficult to trace someone who connects to, say, Starbucks wi-fi. Very basic registration happens, usually around email addresses, and many users would not feel that they need to put full details behind that. The increasing usage of Tor is a particular problem. With Tor, you usually will not see anything at all about the IP address of the destination because each link on the chain is encrypted with a special key so there is no way you can see anything from a Tor connection.

Shabana Mahmood: So tunnelled access—such as VPNs, which many MPs use to log in when they are not on the Estate, for example, and public wi-fi—is becoming the default and therefore not easy to crack.

Professor Bill Buchanan: We have created an internet that is based on legacy protocols. They were created a time when someone had to type in the commands manually. We now have browsers, graphical interfaces and so on. These protocols can be easily breached. They can be sniffed. Anyone who listens to the traffic can crack them. So increasingly businesses and individuals are protecting themselves through the usage of tunnels. Certainly if you are a business you must ensure that your communications are encrypted over public access. If you stay in a hotel room, if you are using the public wi-fi, how do you actually know that the SSID you connect to really is the wi-fi of the hotel? It could be some intruder next door. It happened in the Far East: a whole lot of hackers in a hotel room targeted businesspeople and were continually sending vulnerabilities to them. More and more we are encrypting traffic and setting up tunnels, and it is very difficult for the UK to drive these things because they are typically driven by the cloud providers such as Microsoft, Apple and Facebook.

Shabana Mahmood: On the cloud, people with smartphones go up to the Apple cloud automatically and you get a certain amount of space. Is there any difference in security between the free cloud services and the paid-for ones such as Dropbox, as well as in how much space you get?

Professor Bill Buchanan: Obviously you pay for the security that you get. Brand reputation is very important in this space. Apple, Facebook, Microsoft and Google have their brands to protect. If there was a large-scale data breach for any of those companies, it would decimate them. Banks and the finance industry have invested a great deal in the UK in protecting data and have gone through the CBEST penetration testing. Other companies, such as retail companies and internet service providers, have not gone through the same type of testing.

Erka Koivunen: The question was about future-proofing the legislation. I was puzzled by the introduction of the term "communications service providers"—CSPs. I was not familiar with that. Internet service providers—ISPs—and the telecommunications operators; that is the normal, old-fashioned way of referring to those carrier and access network providers. I was equally puzzled to find that in the actual text of the legislation, CSPs are not mentioned. There are references to what telecommunications operators would need to do and what information would be requested from them. To me, this sounds a pretty old-fashioned way of approaching the problem of acquiring information about content or about whether an event took place in the first place. In that sense, I do not consider the Bill to be future-proof. Because there are so many references to bulk information gathering, it

seems as though there is not even a proper attempt to go to non-traditional telecommunications providers to acquire the material that would be needed. Instead, the information and the traffic would be collected from the wire in bulk and then content or metadata collected with brute force, if you will. Of course, the equipment interference provisions in the Bill acknowledge that whenever you are unable to decrypt the material that you get online from the wire, you will need to go to the end point of the communication, where the material will be stored—hopefully in clear text.

I should point out that our company is actually one of the providers of those VPN type of tunnelling services. We provide a service where you can analyse yourself and encrypt your communication. You are able to move yourself virtually around the world so as to hide the origin of your traffic. Currently, we get only a handful of "targeted" law enforcement requests for the activities of our end users. I guess I am at liberty to tell you that none of them this year came from the UK. In this sense, I am a bit puzzled as to why there is such a pronounced need to get bulk information when even the old-fashioned, more targeted means to acquire information from communications providers are not being used.

Eric King: As upsetting as I am sure it will be if every few years we have to go through a Bill of this length and size, it may be what is required. This is an area that is inherently unsuitable for future-proofing because every year technology simply provides us with possibilities that our laws do not cover squarely or clearly. Where there is a grey area, our agencies have interpreted the law to give themselves the most expansive authority time and time again. Michael Hayden, the former director of the National Security Agency in the US, summarised this by saying, "Give me the box you will allow me to operate in. I'm going to play to the very edges of that box". I am not sure I can criticise him for that. I think that the permission our agencies have is very important and it is right that they use every authority and every capability at their disposal. Nevertheless, it is important that they exercise those powers only when they have been clearly authorised to do so by Parliament.

There have been a number of circumstances over the past few years where in this country we have found that that has not been straightforwardly followed. To my surprise, in the course of litigation involving GCHQ, Charles Farr provided a statement to the court which provided an entirely novel interpretation of what constitutes an external communication. He told the court that if you and I were sending a message using our phones, that would be classed as internal, but as soon as we switched to Facebook, or any other online platform, you and I were no longer communicating. Instead, I was communicating with Facebook, and so were you, and as a result they were external communications. As a result of that, fewer protections were offered to both you and me. It seems to me that that is not right.

We had a similar experience with intelligence sharing. I will not repeat what I know you heard from Amnesty earlier on that point. More recently, I was concerned to learn that, in particular, GCHQ and our security services have taken a very expansive approach on their authorisation of what constitutes a targeted warrant. It seems that thematic warrantry has now become slightly more default than any of us were aware. I was in court a few weeks ago and heard the Treasury devil argue that the use of a general warrant—that is, that you could target on the basis of a class of persons—would be entirely permissible under the Government's current interpretation of the Intelligence Services Act, which they claim

provides them with the ability to hack domestically inside the United Kingdom. These are all issues that the intelligence agencies have thought about. They have determined in secret the scope of their authority, and they are being challenged in these circumstances only because of a whistleblower who brought them to public attention. They have been brought before the courts and they are being tested. It seems to me that we will need regularly to update this law if we do not want to encourage whistleblowers to continue their practices year on year.

Q209 Lord Strasburger: Professor Buchanan, you mentioned the risk if you are in hotel of not knowing whether you are communicating with the hotel's wi-fi or something else. I have been in that position and have had my phone intercepted. It was a demonstration that was organised by F-Secure, so I declare that interest.

On the subject of future-proofing, we have heard many times during these proceedings about the very broad way that various parts of this Bill and other Bills in the past have been drafted. The explanation that we hear from the Home Office is that this is to allow future-proofing so that it can massage the definitions as time goes by. Mr King mentioned this, but neither of the others did. Is the answer to have a new Bill every Parliament, which would be every five years?

Professor Bill Buchanan: I go back to my main point that I can see cryptography and the use of tunnels increasing. There is no Bill in the world that can crack an encryption key that has been created for every connection that you make. You can legislate for it, but technically, it is not possible. The state of the art is 72 bytes. If you tunnelled on every single computer in the whole world, in a month or so, you could just crack a 72-byte key. The keys we are now using are 128 bytes or 256 bytes. It is double, double, double, double until we get to 128. It would take you a lifetime to crack 128-byte keys with current technology.

The Chairman: Is that a yes or a no, Professor Buchanan? Do you think they should be?

Professor Bill Buchanan: I can only say from a technical point of view, from a cryptography point of view, that the Bill would have to provide that cloud service providers would have to hand over the private key, have a key in escrow or have some backdoor, some proxy, on a machine. That is the only way that you would crack the cryptography problem.

Lord Strasburger: I was not talking specifically about cryptography; I was talking about all the provisions in the Bill in order to keep the provisions of the Bill current. Do we need to come back to it roughly once every five years and have a new Bill?

Professor Bill Buchanan: Certainly the way that computing is moving the pace is unstoppable.

The Chairman: Mr King, Mr Koivunen, can you say briefly, as we are beginning to run out of time, whether you agree with Lord Strasburger that we as a legislature should be renewing these provisions every so often because of the changes in technology?

Erka Koivunen: Definitely. I am a big proponent of transparency and the democratic process. Intrusive methods, such as these, should be reviewed.

Eric King: Yes, although I do not think that that should lessen the scrutiny that is put in place for this Bill.

The Chairman: On the principle of renewal, all three of you—or two of you at least are not quite sure—would be in favour.

Q210 **Dr Andrew Murrison:** Do these keys exist, or would they have to be created?

Professor Bill Buchanan: Do you mean the keys of the tunnels that are created or the keys that are held by the cloud providers?

Dr Andrew Murrison: The keys that are held by cloud providers.

Professor Bill Buchanan: A survey was done recently of some of the largest companies in the world. They had an average of more than 17,000 encryption keys—key pairs, as we would call them. A public key is known by everyone, the private key is what you keep secret. If someone finds the private key, they can crack the communications. The majority of companies do not know how many keys they have. Keys are being created at any given time, but companies such as Google will have a master private key which is used for its communications. That key is updated regularly. It might be six months or one year or so. That key will stay active for that amount of time. There is a revocation service on the internet that does not quite work. If the keys have been stolen by someone, what is meant to happen is that all the browsers will no longer accept that key. Unfortunately, Google Chrome does not accept revocation services by default. The keys are actually created by the cloud providers, but every session we create with our cloud services has a new key every time.

Dr Andrew Murrison: I suppose that is our safety net, is it not? We are worried about government having this information, or having access to information through keys. However, the gist of what I am asking is, are we at the moment at the mercy of providers such as Google?

Professor Bill Buchanan: Yes.

Dr Andrew Murrison: Yes, thank you. That is no comfort, is it? There are a number of these, and we presumably have no control over their internal security mechanisms, except as far as their reputation is concerned.

Professor Bill Buchanan: Only 5 per cent of SMEs have any auditing facility with their cloud provider. Only about half of large companies have some form of auditing that they can actually have on cloud services.

Dr Andrew Murrison: Thank you. Can I ask you about definitions in the draft legislation that we have seen? We have a range of descriptions, particularly in relation to communications data, such as entity and events. You might be forgiven for thinking that Sir Humphrey had drafted some of these, because to a lay person they are certainly approaching meaningless. I would be interested in your thoughts on the definitions and whether you think that they are simply creating the aforementioned box and are drafted in such elastic terms as to be maximally obliging to those in the agencies who want to pursue this data. We have mentioned, for example, the thematic warrant. It is not entirely clear to me what a thematic warrant is,

and several witnesses have already said that they are concerned about the fluidity of some of the definitions used in the Bill. I would be interested in your views.

Eric King: As a broad, concerning criticism, the definitions here leave a lot of room for manoeuvre. On issues such as thematic warrantry, it is less the term "thematic warrantry" itself but the scope of the language surrounding that that worries me. The ability in particular to add and remove individuals seems very broad. The more technical terms "events" and "entities", while new to all of us, are not new to the Home Office; they are the terms that GCHQ itself has used for the past decade. GCHQ is very familiar with them and has been exploiting them to the full for a very long time. Events and entities in particular are the issues that are of most interest to our security agencies; these are the capabilities that provide them with the most amount of information. The ISC helpfully said earlier this year that, "the primary value to GCHQ … was not in the actual content of communications, but in the information associated with those communications". I can give you a longer list, but it is very important that these definitions are tightened. A number fall in the gap. As an example, if a telephone call is intercepted and GCHQ identifies the gender of the speaker, is that an event, an entity, content? It is unclear to me.

Q211 Suella Fernandes: Clause 12, Part 2, relates to interception and refers to related communications data. I should say that new Clause 12 replaces the existing Part 1, Chapter 1 of RIPA, so it is a power that already exists. With reference to the point about related communications data, in brief it relates to communications that have been intercepted in relation to the postal service and telecommunications systems, and to assisting with the identification of a telecommunications system, an event or a location. What is your view on the clarity in that clause of the term "related communications data"?

Professor Bill Buchanan: A key aspect of this is that the IP address can never really be trusted, and any digital information that you gain typically from a home environment or electronically, again, cannot be trusted. If someone is in a home environment, they are typically on a private network and they are mapped to a single IP address, so it is very difficult to pick off the person who is actually communicating. So the ability to cross-correlate it with other information, such as location information and calls, is certainly a step forward in providing credible evidence for corroboration. This evidence on its own really should not be seen as an opportunity to look at a single source and to be able to determine the evidence from that. A great worry from our point of view is that within a private network it is very difficult to pick off individuals, so anything that can be added to that certainly helps.

Erka Koivunen: I am an engineer by background. To me, there is only the content, the payload, that we are protecting and then the metadata that describes who was communicating and where the communication was going to. There is other related information such as what type of encryption and network protocol was being used. I read with great interest about the events data, entity data and related communications data which this Bill would recognise, but to me it sounds as though you would need to tap into the network, take all the data and then start peeling the communications so that you could drop the actual payload. Afterwards, when you start dissecting the communications data for law enforcement and intelligence purposes, these terms become relevant, but when the data is acquired it does not matter how.

Eric King: In the interests of time, I will say no more than what I said previously in answer to Andrew Murrison, other than to agree with the best analysis that I have read on this point. It is by Graham Smith, who I believe you have had before you already. I know that he submitted something to the Science and Technology Committee on exactly this question. It was a masterful dissection of a complicated set of questions. I will not attempt to explain it here for fear of embarrassing myself or doing his argument an injustice, but it is one that should be rated very highly.

Q212 Lord Butler of Brockwell: I think you have partially answered this question already, but I will just ask whether you have anything to add. How clear is the definition of internet connection records in the Bill, and is it practicable to get a clear definition that will meet the purposes of resolving the IP identity?

Eric King: The first thing that needs to be remembered about internet connection records is that it is not a term that exists naturally, unlike phone billing records. It is an invented set of ideas. As a result, the first thing we should do before putting new authorities in place is wait to see the outcome of the IP resolution efforts that were made earlier this year with the Anti-terrorism, Crime and Security Act. It is still only months since that Act was passed. Its goal was to provide for IP resolution, which is the same stated goal in this Bill. It is unclear to me why we have not waited to see the fruits of that, to see where the gaps may or may not be, and to learn lessons where we can. The closest I have seen to any state attempting this elsewhere is in Denmark, which had a similar scheme over recent years but stopped it—two years ago, I believe—after it was found to be ineffective. With that, my caution would be to say that we should learn that lesson and wait for any lessons that we can learn from the IP resolution measure that was passed earlier this year.

Lord Butler of Brockwell: Going back to our earlier discussion, is not the answer that this is just a power, so the Home Office could wait for some time before it exercised it? Would you have any objection to this power being in the Bill?

Eric King: I think I would. I am not sure that the blanket retention of communications is a proportionate activity per se. In the Digital Rights Ireland case last year, the CJEU struck down a similar authority for telephone records. My position at the moment is that we should not be legislating at all in this area until cases that are going up to the CJEU are resolved, for fear of us all wasting quite a lot of our time and having to re-amend and re-adapt the law, particularly given that we could be waiting to see how the Anti-terrorism, Crime and Security Act is implemented. I think we should hold back in this area and not include it in the Bill at all.

Lord Butler of Brockwell: Do your colleagues have anything to add on ICRs?

Erka Koivunen: I would like to continue with a Danish example. I have been told by my old Danish colleagues at DK-CERT that there was an attempt to mandate that all public wi-fi providers should be required to keep session logs of where their users were communicating to. This would include not only telecommunications operators but cafés, conference halls and airports. I used to work for a telecommunications provider and we used to call these cafés hobbyists. These hobbyists would be required to gather sensitive information about who their users were communicating with and they would need to retain that information and have it available whenever law enforcement requested it. To a cybersecurity

professional, that spells disaster. It is a disaster waiting to happen. Each and every store of this kind of information would be a target for computer intrusions by criminals and foreign intelligence services. One also has to remember that it would be pretty expensive for the service providers to start collecting that. In Denmark, in the end, that is why the so-called hobbyist providers were exempted from that legislation, and eventually that whole law was scrapped.

Professor Bill Buchanan: I go back to my point that proxy systems hide the IP address of the sender. Tunnelling systems hide the content. Tor systems hide the content and the IP addresses of the sender and the destination. VPNs hide the content and the source address. Many people are moving to cloud-based systems: you can run virtual desktops within the cloud. The concept of running things on hardware is going. We are moving towards almost a mainframe-type system. We have a terminal that we connect to the cloud and the cloud exists somewhere else on the internet. Anyone who is even a little bit tech-savvy is able to pick one of those systems and hide their logs. Providers need to think through all the options and collect other information which can then be used to corroborate with the pinpoint of information that you might get from an internet service provider.

Lord Butler of Brockwell: So you would conclude that, in its present form, this is not value for money?

Professor Bill Buchanan: In its present form, from a technical point of view, it can be very difficult to find the information that is actually required from purely internet-based records. There is a whole lot of other information that we leave behind. If we have a mobile phone we can be tracked every time we make a call, and so on. There is a whole lot of other information that could be used alongside the internet record. This is not the catch-all that it could be. Ten years ago it was: you could look at anyone's record. The one company that has the whole record of every little thing we have done on the internet is Google. It has all our information. That is because it is the end point. It is the place that you go to and it will see all the information. Unfortunately, that jurisdiction is not inside the borders of this country.

Q213 The Chairman: Clauses 51 to 53 of this very long Bill talk about a request filter. What are your views on that?

Eric King: If I may, I would like to get back to the Committee on that, once I have some questions clarified by the Home Office about the exact scope of what it intends. My starting point is that it permits the same sort of data-mining at a scale that so far only our intelligence and security agencies have been undertaking, and provides that to the police, but in the name of a safeguard. Regrettably, a more detailed analysis requires more information but I will be very happy to provide the Committee with that once it is available.

The Chairman: Would you like to comment on that?

Professor Bill Buchanan: It is certainly a good way forward. Some sort of definition of the search terms that would be used would protect us from a large-scale data breach. The last thing we need is for all the information from an ISP to be leaked because a log was allowed to be taken of its site. The logs should be kept in a trusted environment and the access to them should be locked down to IP addresses and to biometrics if possible. Because they

are probably among the most sensitive logs that we have, if we make sure that the requests made actually match what has been collected, we can make sure that a summary record is given to law enforcement, not the full record. Systems are easily breached. You can take data quite easily from them. It is very difficult to protect them. An abstraction around a request filter is a good way forward.

Q214 Lord Strasburger: Is it reasonable and practicable to require communications service providers to remove the electronic protections from their data when providing it to law enforcement agencies and the security and intelligence services?

Eric King: This issue has taken on increased importance due to how it seems that the Home Office wishes to apply it in future. If it intends to use it to force companies such as Apple to remove encryption or to re-architect their systems to provide a backdoor, that would be wholly inappropriate. It would provide a lesser degree of security for us all. The Home Office needs to answer many more questions as to how it intends to use this authority. If the companies' public statements on this issue are to be believed, we should all be concerned.

Erka Koivunen: From a technical point of view, if the telecommunications operator which has been served this kind of information request is able to remove those protections, which are typically provided through encryption, of course it would make sense for these protections to be removed to enable the law enforcement and intelligence agencies to make any use of the data that they receive. However, echoing what Mr King said, there are many stakeholders in these communications service providers. Some of these providers have designed their systems specifically to employ end-to-end encryption, where the service provider is not in a position to open up the encryption. The encryption goes through the service provider's systems so that even the provider is not able to see through it. The way I am reading the Bill, it would actually ban the use of strong cryptography and strong encryption and would essentially weaken our ability to use secure online services.

Going back to the question of future-proofing, as a company that provides systems where we potentially are not able to decrypt the traffic that we pass—

Lord Strasburger: Sorry, did you say "are" or "are not"?

Erka Koivunen: We provide services that we would not be able to decrypt ourselves. We are not sure whether the Bill would concern us—whether we would be compelled to redesign our systems. I imagine that Apple will be reading the Bill with a similar sentiment. I think that it would refuse to redesign its systems in a fashion that would open up and weaken the encryption. So the Bill has some problems in the way it has been written.

Professor Bill Buchanan: Cryptography and the methods that we use in cryptography are almost perfect. Unfortunately, it is the humans who implement it who are flawed. The humans who implement security, too, are often fairly flawed in their approaches. If you ask most people whether they trust that their ISP's or CSP's security is robust enough to handle secure information such as this, I think the majority would say no, especially after the TalkTalk hack. I have many examples of where they use weak passwords and so on. If we have now got to the point where our banks can be trusted with data because of the CBEST standards and can be put to the onerous task of protecting records such as this to provide

lots of different levels of access, then the ISPs and CSPs have to up their game many times over. They have typically grown from telecoms providers and have been merged from lots of little companies to provide big, heterogeneous types of organisations that are difficult to control.

The only way is with multifactor authentication. The idea that you can open up some data or a log with a single key or a single password has gone. The controls and the proving of identify is key to providing access to the data. The data should never appear offsite at all. The only way you should be able to access the data is by remote access and only through a portal. If we were to risk the opportunity of downloading a whole aggregated log on to a machine with a single encryption key then we really are opening a can of worms. CSPs and ISPs need to be thinking about access. Certainly there should be some biometrics in there—fingerprint recognition at least, along with geolocation, so that only certain locations would be allowed access to it. A mobile phone, through out of band identity methods, is also a good way. You really must wonder, "If my password is changed by my mother's maiden name on my ISP, anyone can find out my mother's maiden name fairly simply from an internet search". If that is the level that ISPs and CSPs are now at, they need to recruit a whole lot of security engineers, architects, cloud engineers and so on. They need proper investment because this will be a massive task. The banks are soaking up all of our graduates to work in these types of environments. The next wave is that if the UK cannot produce enough cybersecurity specialists, where will we get all these new specialists? The country needs to think ahead and, I hope, invest with the ISPs or CSPs to make sure that they protect our data.

Lord Strasburger: What are the risks and benefits of allowing law enforcement and the agencies to undertake equipment interference? I mean both types of equipment interference, targeted and bulk.

Eric King: On the law enforcement side, the most powerful argument I have heard for preventing law enforcement having access to equipment interference was from the Suzy Lamplugh Trust earlier: the powers they are currently provided with are not being used to their fullest. Given the incredible intrusiveness that equipment interference could provide law enforcement, we should treat it with extraordinary scepticism. One of the issues at the front of my mind and which I have not had an answer from police or the Home Office on is how we will get around the issue that, by deploying equipment interference—what the agencies sometimes call "computer network exploitation"—we will not damage evidence that the police would later wish to seize and rely on in court. It seems that it would be incredibly counterproductive to be providing an authority in this manner that, in some circumstances, could result in criminals getting off the hook. Until I hear a compelling answer from the Home Office on that point I am not sure that we should move forward with that aspect.

In the intelligence domain it is far more severe. I struggle to understand exactly what the Government have in mind by bulk equipment interference. Every single scenario that I can conjure up seems to be within the scope of what are the not very targeted but nevertheless called targeted equipment interference powers that are there. That is because it provides them with thematic warrantry or even hacking by location. That by itself is very broad. We need to understand that, by undertaking interference, our agencies threaten British

cybersecurity. They regularly hack companies in Europe and elsewhere that are not a national security threat in and of themselves. The employees of those companies are not suspected of any serious crime or criminal wrongdoing, but these companies are being attacked to allow GCHQ and other agencies to undertake further attacks. In recent years, we found out that GCHQ hacked Belgium's largest telecoms provider, Belgacom. It has also hacked Deutsche Telekom, Seagle, Stella—the list goes on and on. In doing so, they are painting targets on British companies' backs in exactly the same way and legitimising these kinds of attacks. By attacking using vulnerabilities in networks and systems that they have acquired themselves but are refusing to tell the world about so that those companies can protect themselves, they reduce the security that we collectively experience. The stockpiling of these vulnerabilities in zero-days is not considered in the Bill. Policies need to be very clearly set out about it before any consideration is made of the powers. As it stands, our recommendation to the Committee is that bulk equipment interference should be absolutely prohibited. There seems to be no good reason why such a thing could be undertaken. Should equipment interference be permitted at all, I point the Committee to the recommendations made by Privacy International and the Open Rights Group as a result of the draft equipment code of practice introduced earlier this year in response to recommendations.

Lord Butler of Brockwell: May I ask one short supplementary on that? You say that we are putting British companies at risk by pinning a target on their backs. Foreign interceptors are not going to intercept British companies just by way of revenge, are they? They will do it anyway if they want to.

Eric King: I would hope not. Nevertheless, by using vulnerabilities and imagining that we are the only state that has discovered them we allow British companies to continue to be exposed to those threats. Instead, when British agencies find a vulnerability in networks, their presumptive position should be to disclose that to the appropriate vendor so that all companies can benefit from that security. Instead, by keeping them and using that as part of attacks, we first raise a flag, so that when those attacks are eventually discovered others will use that same attack here in the United Kingdom. Secondly, we are preventing them from being able to defend against attacks that we could be assisting them in preventing in the first instance.

The Chairman: We are getting very close on time now.

Erka Koivunen: The term "equipment interference" is pretty elegant. When I was learning information security at school we used "exploitation", "vulnerabilities" and "attacks" to describe the same things. There was no discussion of vulnerabilities or attempts to let the vendors of software products know about them. Equipment interference also refers to the deliberate introduction of those vulnerabilities and backdoors in products. In recent days, we learnt that Juniper, a big provider of core networking components that the internet is being built on, found backdoors and means to weaken encryption in its systems. This backdoor was in its code for at least two years. This was probably of use to some intelligence organisations' operations around the world. However, the UK networks, the Finnish telecommunication providers' core networks and the corporations' networks are being built by the exact same systems. They have been vulnerable to this type of exploitation for two years already and are not rushing to patch their systems. Cisco Systems

had a similar case a couple of years ago that was not publicly discussed. There are many systems where it has been suspected that vendors have been compelled to introduce backdoors of this nature to deliberately weaken cybersecurity protections in favour of some intelligence organisations. I see this as a threat to civilian society's ability to conduct business online, and to e-government processes. When we cannot trust our information-processing infrastructure, we tend to avoid using it to conduct business.

The Chairman: Very briefly, Professor.

Professor Bill Buchanan: My view is that virtually everything is possible and it should be based on a risk-based approach. If something is high-risk these things should actually happen and we should be looking at exploiting vulnerabilities. As long as there is a reason for doing it and it is documented and audited, really anything is possible from a technical point of view.

The Chairman: Thank you very much indeed. Mr Warman, you have a final question before we move on to the next session?

Q215 Matt Warman: I should declare that my wife is a student at Queen Mary, but not one of yours so do not worry. If we look round the world, how does this compare to international legislation that is coming forward or is currently in force?

Professor Bill Buchanan: In France just now the access to public wi-fi is being looked at. In Kazakhstan, of all places, they are looking to implement a digital certificate where you cannot connect to a secure channel unless you use the Kazakhstan certificate. Unfortunately, the problem with that is that none of the cloud providers trust that certificate, which means that it could decimate their business and the social aspects. It has been done with the aim of improving privacy but there may also be a political agenda. It has also been shown that general certificates can be hacked. It happened when Iranian hackers got access to the DigiNotar certificate, which was a Dutch certificate, and managed to hack 300,000 users on Google and listen to their communications. Most countries are now looking at the inability to view logs. Few countries have been able to get the balance right.

Erka Koivunen: As a matter of fact, I am participating in the reform of the Finnish intelligence legislation and there are discussions about targeted equipment interference, using the terminology in this Bill. There is a pretty wide consensus that attacking foreign military installations will be something that we will see parliamentary consensus on next year, when it goes to parliament in Finland. The intelligence services in Finland have already publicly stated that they are refraining from demanding backdoors and the weakening of encryption while they seek a new mandate.

Eric King: There are lots of comparisons we could look to but we should focus on the United States as a country that we share a very similar capability with; under the Five Eyes Alliance, we also have much the same approach to issues. Over the past two years in the United States, reforms have been made to curtail NSA capability. There is one power in particular that I bring the Committee's attention to, and that is to do with bulk communications data acquisition. This is what was avowed by the Home Secretary to the Commons when introducing the Bill. While we have very little information about how this is used in the UK,

in the United States this was on the front page of most newspapers. Very helpfully, two independent bodies that had access to classified material were able to look at the programme and consider it in detail. The President's Review Group on Intelligence and Communications concluded that the use of this was not essential to preventing attacks. Similarly, the Privacy and Civil Liberties Oversight Board concluded that, "we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot". This is a power that there have been two detailed reviews on in the United States and that they have decided to end. Indeed, it was just a few weeks ago that that programme was brought to a close but here the Bill is attempting to place it on a statutory footing for the very first time.

Matt Warman: That is not a technical point—if our agencies were to say that they thought it was necessary for national security, there is not a technical argument for making the observation that for political purposes or whatever they have made a different decision in a different country?

Eric King: In the country in which an operational case was made, that could be scrutinised by a series of very senior experts—who in many circumstances were very close to the intelligence community—who had access to classified material, who looked in detail at the operational case and found it lacking. My presumption is that the Committee should take the same approach until such a time in which the security services provide a public rebuttal and can show that the operational case is somehow different from the one that was so carefully scrutinised by so many people in the United States.

The Chairman: Thank you very much, all three of you, for a very interesting session, particularly Erka for coming a long way at relatively short notice. We wish you a very happy Christmas.

Colin Passmore, Senior Partner at Simmons and Simmons, on behalf of the Law Society (QQ 137-144)

Evidence heard in public Questions 137-144

Oral Evidence

Taken before the Joint Committee

on Monday 14 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Stuart C McDonald MP, Matt Warman MP, Baroness Browning , Lord Butler of Brockwell, Bishop of Chester, Lord Henley, and Lord Strasburger.

Witness: **Colin Passmore**, Senior Partner at Simmons and Simmons, on behalf of the Law Society, gave evidence.

Q137 **The Chairman**: A very warm welcome to our witnesses today. I know there was not very long notice for everyone, but thanks to all four of you for coming along to give your thoughts on what is regarded as probably one of the most significant Bills of this Session. As in previous sessions and in any similar parliamentary committee, we will ask you a number of questions, which I hope will stimulate your brain cells. We will have a dialogue with you in this particular session about the importance of privilege to the legal and journalistic professions.

I am going to start by asking a question about the legal professional privilege. How do you think the draft Bill addresses the concerns of the legal profession about privilege and the investigatory powers in England, Wales and, of course, Scotland? Does it create any new issues?

Colin Passmore: It falls to me, as the lawyer among the four of us, to see if I can address that. My name is Colin Passmore. I have been a solicitor for 31 years now and I can modestly claim to be an expert on privilege because I write the leading textbook. I am sad enough to know the thousands and thousands of cases on privilege and the hundreds and hundreds of statutes that deal with privilege. What is unique about RIPA and this Bill is that, on the face of it, they do absolutely nothing to address the concerns that the legal profession has about privilege and the way in which surveillance techniques in all their glory can be used to infringe the privilege.

Privilege, as I am sure you know, is possibly the highest right known to the law. It is over 500 years old. It is jealously guarded, not only by the legal profession but by the courts, with the result that there are usually hundreds of cases in London alone every year in which challenges to privilege are upheld. In addition, in every single statute that confers investigatory powers of any sort, whether we are talking about the police, the SFO, the Revenue, even local weights and measures departments, there is always a provision that actively protects privilege, so nobody—the police, the Revenue—has the ability to force any client to divulge their privilege. The same thing happens in statutory instruments. This

draft legislation and its predecessor are unique in that there is nothing in them that protects privilege.

When this issue came before the House of Lords in the McE case from Ireland some years ago, it is fair to say that the legal profession was extremely surprised that Section 27 had the ability to enable the security services, the police and others at least to listen in to privileged communications in certain circumstances. Even the House of Lords in that case indicated a great reluctance to interpret Section 27 as giving the ability to listen in on privilege, but the House of Lords proceeded quite clearly on the basis that this happens very, very rarely. The House of Lords was at pains to say that if it happens on a regular basis there will be a chilling effect on privilege. The chilling effect is really important, because it inhibits the frankness of clients, whose right it is, with which they speak to lawyers. If that chilling effect is in play, it could undermine the right to a fair trial under Article 6, infringing on privacy rights under Article 8, and undermining the administration of justice.

We know now, from cases like the Belhaj case and other cases that have come to light in the last year, that whereas we thought this interference with privilege was very, very rare, it is happening far too often and on a routine basis. In my view and the Law Society's view, unless this legislation is amended so as to deal with privilege on its face, then privilege, this very old and supremely unique right—there is nothing else like it in any form of communication—begins to become seriously undermined.

The Chairman: Mr Musson, do you want to add anything to that?

Tim Musson: Not a great deal, Lord Chairman. My background is not legal professional privilege in the same way as Mr Passmore's. I am here to represent the Law Society of Scotland. It appears that legal professional privilege in Scotland is very similar to that in England and Wales. The differences are absolutely minimal, although it has arisen in a slightly different way. There are the two sides to the privilege: England started on one side, Scotland started on the other side, and they have come together. Certainly the Law Society of Scotland is very concerned about the erosion of legal professional privilege that appears to be quite possible with this Bill. They have great concerns about it, which do not differ in any way from what Mr Passmore was saying.

The Chairman: Picking up on where Mr Passmore finished, and now that you have added to his comments, it is very appropriate for our only Scottish member to come in on the issue of any possible amendments.

Q138 Stuart C McDonald: Mr Passmore, you suggested that this Bill will need some amendments before you are happy with its approach to privilege. Can you give us any more indication of what sort of amendments you think would be required?

Colin Passmore: There is a serious question as to whether there should be a prohibition on interference with privilege at all. Why is this interference necessary? I respectfully suggest that there are not many cases where lawyers, be they solicitors, barristers, advocates, have been found guilty of abusing the privilege. If a solicitor or a client in their relationship with a solicitor abuses the privilege, the privilege falls away. There is something known as the crime-fraud exception or the iniquity exception.

You do not need these seemingly open powers to listen in to solicitor-client conversations unless you have some evidence that there is something wrong going on. There is very little evidence that solicitors or lawyers abuse the privilege, and therefore the power to listen in, to intercept or to hack is simply, in my view, unnecessary. I would be a strong advocate, and the Law Society is a strong advocate, joined by Scotland and indeed other jurisdictions, for having the type of privilege preservation clause that you find in all other statutes, including those that deal with police powers, revenue powers and so forth. I respectfully suggest that there needs to be a provision in here that makes it clear privilege is out of court.

Stuart C McDonald: Are you frustrated, then, that sometimes we hear from the Home Office that they are scared of putting some kind of prohibition on intercepting legal privilege because of the risk of abuse? You are saying to us in effect that that abuse means that the privilege no longer applies.

Colin Passmore: That is my view. I know many lawyers who understand the importance of privilege and its unique status as a means of privacy in communications with clients. Many lawyers whom I know take the obligations that arise from having the benefits of privilege very seriously. I can think of a handful of cases in which privilege has been abused; I am aware of one, which came to my attention this morning, that has just gone up to the European Court of Human Rights. It simply, in my view, does not happen that lawyers abuse the privilege.

Stuart C McDonald: Mr Musson, do you also seek that prohibition in the Bill?

Tim Musson: Ideally, yes, I would seek that. If it cannot be taken as far as that, there become issues about who is competent to permit interception of these communications. It would need to be someone who understands legal professional privilege, and the sort of person involved in this authorisation might not have that knowledge or understanding.

Q139 Lord Butler of Brockwell: Mr Passmore is making the case for prohibition on the grounds that privilege falls away if a lawyer is engaged in criminal activity. In those cases, you would say that there must be evidence that that is happening, but then you are putting too much power in the hands of the authorities, are you not? They say, "We have evidence"—let us say this is the Home Secretary—"and, therefore, please may we have a warrant to listen to this lawyer because we think privilege has fallen away?". Would you not rather have a stronger safeguard than that, a formal procedure that certifies that that is the case, rather than just the judgment of the Executive?

Colin Passmore: That is a good point. I do not make the case just on the basis of the iniquities exception. I make the case primarily on the sheer importance to the administration of justice of the privilege itself. I am very concerned that this Bill has the ability to undermine privilege more generally. With regard to your second point, in the way this iniquity exception works with, for example, the police, the SFO or the Revenue authorities, when they seek a warrant to go into a solicitor's office, they have to satisfy the judge in the Crown Court that there is a really good case for being able to go into the solicitor's office, knock on the door and start to take papers away.

Forgive me, I am going slightly off your point but I will come back to it. If privileged materials are identified, whether or not the exception applies there is always an independent lawyer in attendance who will do the physical bagging up of the documents or the computer disks, and he or she will later go away to determine whether they are privileged. There should be a check, of course, but a judge is more than capable of looking at the evidence as to whether or not the iniquity exception is likely to apply. Judges are very good at this.

Lord Butler of Brockwell: Would that not be covered by the new procedure under this Act: that if the Home Secretary is to grant a warrant, it has to be endorsed by a judge?

Colin Passmore: Yes, as long as the reference to the judicial review standard is removed—first, because that introduces an element of ambiguity: what is the judicial review standard? I know that eminent lawyers such as David Pannick have written to say that it is fine; I know many others who disagree with that. But I am not even sure why we need that. If the communication that the authorities wish to intercept is subject to the iniquity exception, that of itself should be enough; we do not need a judicial review standard. Does the exception apply prima facie or does it not? If a judge is not happy that the exception applies, the warrant or the ability to intercept simply should not be granted.

Lord Butler of Brockwell: That, if I may say so, raises a slightly different point. I am not trying to put words in your mouth, but I think you are saying that if the judicial review test was removed, you would be content with a procedure whereby the Home Secretary can grant a warrant, provided it is endorsed by a judge, if there is a really good case?

Colin Passmore: Coupled with an express recognition in the draft Bill, in the statute, that privileged material is not available, that would be great. I would be happy with that and I think the Law Society would be.

Bishop of Chester: The closest parallel might be a confessional and a priest. It is humorous on one level but serious on another. It is on a much lower level than legal privilege, but what qualification there is to an iniquity exception is a matter of contemporary discussion. It may apply only to the Church of England, but we have other religious groups in our country now. I would have thought that if we are going to put something in the Bill, in principle we should, I suggest, at least look at whether that is a parallel set of circumstances, because putting a bugging device in a confessional situation raises the same sort of issues in a different context.

Colin Passmore: It does. I am sorry to disappoint you, but the law addresses privilege as a higher right capable of greater protection than the confessional box. It is easier to get disclosure of your conversations with a confessor than it is my conversations with my client. I am not saying it is very easy; it is very difficult, but I am afraid privilege is on a slightly higher plane so far as the English and Scottish courts are concerned.

Victoria Atkins: To clarify, on the point of the iniquity exception, your evidence is that you wish protection to be put into the Bill that reflects the law as it stands currently across all other statutes, so if a solicitor is trying to commit a crime with their client, that information will not be protected by privilege?

Colin Passmore: Absolutely right. It cannot be protected.

Victoria Atkins: You gave the example of search warrants. Interception warrants are a much rarer event even than the pretty rare event of HMRC or whoever going into a lawyer's office. The safeguards are there, surely, for interception warrants, given how rarely, particularly in secure environments and so on, these are used.

Colin Passmore: The occasions that we know of when cases in which the police have sought interception warrants have come before the courts are relatively rare, and you have to go through the Crown Court judge warrant procedure and satisfy the judge that the iniquity exception is likely to apply. I am a long way from being an expert on interception and the security services, but I have been slightly horrified this year at the number of cases, starting with Belhaj and others, that have come before the IPT in which these issues are raised. I am not myself convinced, although I am not an expert—far from it—that these cases are such a rarity. I would therefore far rather the security services et al had in the Bill the clear recognition of just how important privilege is, plus the mechanism of going via the judge.

Q140 Suella Fernandes: Thank you for your evidence today. Do you agree that someone who belongs to one of these professions that we are talking about, maybe the legal profession or the journalistic profession, may also, albeit in rare cases, pose a threat to national security, and in those cases it is important that the agencies have a power to intercept their communications?

Colin Passmore: I find it difficult to think of a case that would be any more than a rarity. I am aware of one case in Northern Ireland, which is the case I alluded to earlier that has just gone up to the European Court of Human Rights, where a solicitor conspired with his alleged terrorist client to bump off a witness. That is incredibly rare. It is so rare it is shocking. I am not aware of any cases where that is likely to happen. I am not suggesting for a moment that every single member of the legal profession in the UK is beyond reproach—of course not—but I find that a difficult concept to get my head around.

Suella Fernandes: Do you appreciate that the agencies have given evidence that they would never specifically seek to acquire privileged material except when they apply for a specific warrant?

Colin Passmore: I would give you the lawyer's answer to that, inevitably, which is that if that is the case, they cannot have a problem with the Bill recognising the importance of privilege. In other words, if they recognise that they do not want privilege, let us put it in here and make sure it is beyond doubt. Then, if there is a circumstance in which the iniquity exception applies, go to your judge for your warrant. If your evidence is good enough, fine, you are up and running.

Suella Fernandes: Lastly, it is always subject to the test of being necessary and proportionate and that the intelligence cannot be obtained in a less intrusive way.

Colin Passmore: That I disagree with. The courts and some very famous names in the judiciary, such as Lord Denning—I am showing my age—and others since have recognised that the consequence of a claim to privilege is that the court, the Revenue and the police are deprived of what they regard as potentially relevant evidence. It is a consequence that we have to face with an assertion of privilege.

Bob Satchwell: I think your question was: could it be possible? It would be foolhardy of me to say that it was impossible, but it would be astonishing. There are so many examples of the way journalists understand and very carefully apply restrictions upon themselves in relation to national security issues through the DSMA committee, through what were wrongly called D-notices, and things like that. We work like that all the time. I have never known of a journalist who would ever have put someone's life or national security at risk inadvertently. What we are concerned about is precisely the point that there need to be very clear procedures and rules if someone is seeking to invade the journalist's activities and his sources. More recently, and perhaps we will come on to this, the evidence has been that some organisations rode roughshod over something that we all thought was accepted.

Q141 **Victoria Atkins**: What is the legal status of the codes of practice under RIPA?

Colin Passmore: Vague. They are the worst option for dealing with this issue, in our view. We have a problem here at the moment in that the codes of practice that will be developed pursuant to this are so far unwritten, although I imagine they are going to reflect a lot of what is in the present codes. A code of practice is what it says on the tin: it is a code. We have seen from recent cases where the security services have breached the code that there is not really a sanction. There may be some disciplinary sanctions, but we have seen that the remedies available in the ITP are pretty low-key compared with what one might expect to get, for example, in the High Court, where there might be a claim arising out of a breach.

They are clearly not of the status of legislation. In the absence of something in the Bill, something in the Act to be, that makes the status of privilege clear, the code of practice is always going to suffer, in our view, from this weakness that cannot be cured, no matter what you put in it. It is a code. It is slightly better than the *Highway Code*.

Victoria Atkins: Should we not separate between security services and law enforcement on this issue? As you know, under the codes of practice for the Police and Criminal Evidence Act, there are very real ramifications for the prosecution if the police fail to follow the code. The case may be dropped.

Colin Passmore: I totally agree, but the big difference is that the Police and Criminal Evidence Act, or the Criminal Justice Act for the SFO, makes it clear that privilege is untouchable. You have this primary legislative direction that we do not have here, nor with RIPA. Therefore, the codes of practice are bound to suffer from that. The codes of practice currently have all lovely things about privilege, but they are effectively unenforceable. You have to trust the operatives in the security services to make sure that they will obey them and that they will adhere to them. Personally, I do not think that is good enough when we are dealing with privilege, which as I keep saying is this extraordinary right, which should be protected in the primarily legislation.

Victoria Atkins: What do you expect to be contained in the codes of practice issued under this Bill?

Colin Passmore: That depends what is in the Bill. I would like to see in the Bill: a recognition that privilege is untouchable and that therefore there should be a fair amount of guidance to the security services and others on what privilege is, why it is so important and what the consequences are of coming across it: a very clear statement, if I may suggest, that there is

no basis whatsoever for targeting it deliberately; a very clear explanation of what the iniquity exception should be; and a very, very clear statement of the dangers of playing fast and loose with privilege. You may ultimately cause a trial to be stayed because you have interfered with a defendant's right to a fair trial; you have interfered with his or her privilege. There would need to be a lot, in my view, in the code of practice. I do believe that it has to emanate from the primary direction in the Bill as to the importance of privilege.

Victoria Atkins: I have a final question on that. The commissioners will play a very important role under the draft Bill as it stands at the moment. Is it not sufficient to trust them with bearing that very much in mind when they are looking at individual applications, and in due course reviewing how the legislation is being applied generally?

Colin Passmore: The intent of the legislation is that there would be a senior judicial officer, at least at Court of Appeal level or above, so really senior, experienced lawyers. Provided they also have the direction in here that privilege is untouchable unless the iniquity exception is in play, I would be happy with that.

The Chairman: Thank you very much. We turn now to journalistic provision and privilege, touched on Clause 61 of the Bill.

Q142 **Suella Fernandes**: Clause 61 requires that a judicial commissioner approves the issuing of any warrants for obtention by agencies. What is your view of that safeguard in protecting the media's rights?

Bob Satchwell: Our simple view is that it does not go far enough. Some interim measures have been put in place to do with RIPA and so on, but the difficulty is that RIPA was used—I have always argued that it was misused, actually—in certain cases, some of which became very full of headlines and so on, to get around the good safeguards that are in PACE. A number of examples that learned lawyers have come up with—I am not a lawyer, by the way—show that that happened.

The key point with legislation of this kind is that we know what the basic intention is in these troubled times, but that is why legislation was enacted previously. I remember when RIPA was enacted it was made clear to me by Ministers whom I talked to, and I believe it was the will of Parliament, that RIPA was supposed to be an Act to do with fighting terrorism. We have found that, in fact, it became something completely different.

I start by saying that it is very important that the legislation—with all due respect to those who may have been involved in that legislation originally; no one expected that it would be misused in the way it came to be misused—is very clear what the ground rules are before you even get to the codes of practice. Codes of practice are fine so long as someone follows those codes of practice. It absolutely needs to understand, as most people understand—it is something I have always had in my mind, and I have been 40 years a journalist—the first rule of journalism: that you protect your sources. That is in other parts of legislation. It is understood in Europe. It is understood in most places. Judges will very rarely make a journalist reveal his sources, and so on. That background has been totally misunderstood by the police for example, who have ridden roughshod over those principles. Somehow it has to be there very, very clearly.

Going back to your previous question about the possibility of a journalist being involved in something that was against the national interest, they have to come up with evidence, not a fishing expedition; it has to go before a judicial authority. What is more, there has to be an opportunity for the media organisation to argue and to explain the case, because it is not just a matter of delving into journalist records or into who those sources are.

An inquiry into certain parts of a journalist's activity may inadvertently reveal a source that the police or the security services are not interested in. That is why it is very important that there is an opportunity to know when the police or the security services are asking for that, and an ability to argue that case.

The Chairman: Mr Smith, do you want to comment?

Andy Smith: Yes, just to pick up and elaborate on a couple of things that Bob has said. The NUJ agrees that, while not ideal, the provision under PACE is one that we have been able to work with. We have been able not only to oppose some applications outright but to use the knowledge that we have as journalists to explain the situation that we are in, so that a judge can make a variation of something in front of him, which, as far as I can see, is very difficult under the framework that you have in front of you. A police force may come and ask for hundreds of hours of video tape and end up with 10 or 15 seconds that the judge considers to be pertinent to the application they have made.

To be clear, what we have under PACE, as Bob said, is: prior notification, which we think is absolutely essential; sufficient information about the application, for instance what other means have been attempted to obtain the information, so that we are treated not as a first resort but as a last resort; the importance of a face-to-face hearing, which is not about journalists having their day in court but about being able to demonstrate, particularly to potential sources of information, that the journalist's commitment to protect their sources goes up to defending them in open court and going to bat on their behalf; and a rigorous right to appeal before approval is granted. Under the draft legislation, there is an ability for the force or body making the application to appeal, but there is no right to appeal for any of the persons affected, simply because they are not told.

The only other point I would make initially is on the business of communications data, as opposed to the information contained in the communication itself. Journalists are in a very particular position, in that very often the information gathered has already been published and the most important thing is the fact of the communication. The communications data is at least as important as the content of the communication, quite possibly even more so, given our commitment to protect journalistic sources. It is a very particular situation that journalists are in in that respect.

Suella Fernandes: I have one final question. Special protection requires special responsibility, and in some professions the communications between the professional and their client are very well-regulated, for example the medical profession or the legal profession. There are regulations covering journalists, but they are very different from the regulations that apply to the other professions. Do you agree with that?

Bob Satchwell: Yes. It is quite reasonable. Journalism is not a profession in the sense that the professions are professions. It is not a closed shop in that sense.

The Committee suspended for a Division in the House.

Bob Satchwell: But I hope that we always act professionally, which is somewhat different. In all the codes of practice that journalists have, whether for newspapers and magazines or in broadcasting and so on, there is a simple recognition that the protection of sources is a moral duty, as it is put. That is recognised by the courts, by European authorities and so on.

Andy Smith: The other thing PACE does is concentrate on journalistic material. If a journalist, however they want to label themselves, is doing anything that is outside of that journalistic function, it is not covered. Bob talked about the times when legal privilege falls away, and, in a similar way, material that the police want to access concerning a journalist doing something other than their job would not be covered.

Suella Fernandes: The point I want to make is that there is much less regulation for journalists compared to the other professions, and the definition of a journalist is not as clear cut as it is for members of the legal or medical professions.

Bob Satchwell: That is true, but just because the regulation is not quite as formal does not mean that it is not followed. In some circumstances, the following of journalistic practice, which is accepted across the industry, is stronger because it is not laid down in legislation. The fact that it is peer judgments means that people will adhere to it.

On the question of sources and the release of information, it has been recognised in legislation and it is recognised in the courts that sources and other journalistic material should be delved into only in special circumstances.

Q143 Matt Warman: I should declare an interest. I am a member of the NUJ, although, I suppose, a recovering journalist. To start off with, what is a journalist these days? Would you include bloggers? Would you include someone live-tweeting this Committee who is effectively a member of the public? Where might we draw that line?

Andy Smith: To go back to what you were saying, there is an interesting debate to be had on that. I have seen various definitions. The advantage of PACE is that it does not define a journalist, and in some ways that is safer. If that definition is to develop as the technology develops, I would rather see that debate happen as a matter of developing case law, which would involve open hearings rather than conversations behind closed doors that make decisions arbitrarily, or not arbitrarily, about whether somebody who, for instance, had a regular blog and followed our own code of practice but was not paid for it would be described as a journalist. Frankly, some very good journalistic work is being done on the internet by people who are not associated with the traditional media outlets. There is a debate to be had there, but I would say it is developing.

Bob Satchwell: There are probably some common-sense definitions. It is difficult to define now, but, as Andy said, it will be developed in law. That is one of the reasons why there needs to be an ability to argue a case and say whether this person is a journalist or not. That is part of the principle that is there. I can see that some authorities would say, "We did not know he was a journalist. We just did it". That is the difficulty: that people will try

to go outside what has been accepted practice in the past. It would be difficult to define absolutely what a journalist is.

Matt Warman: Bearing in mind that as-yet-undefined elasticity, how could we amend the Bill in front of us to achieve some of the things that you are talking about?

Bob Satchwell: There will be a submission from the Media Lawyers Association, which will come back in huge detail on this. Please excuse me for not having all that legal background. They will come up with some very clear suggestions on that.

Matt Warman: Mr Smith, did you want to add anything to that?

Andy Smith: Like Bob, I am not a lawyer. I would not want to start amending it for you, but the principles would involve something like "somebody who is regularly practising" or "employed". Those sorts of phrases would allow you to separate out those who are simply expressing an opinion on a blog on a regular basis from those who are engaged in journalism.

Q144 Mr David Hanson: Could you comment on what happens when a journalist is undercover and is acting as a journalist but is not, to the public knowledge, acting as a journalist at that particular time? The fake sheikh has been mentioned, but there may be other examples that we are aware of. I am interested, again, in the definition in relation to the Bill.

Bob Satchwell: In most cases, they will be employed or commissioned to be doing something undercover, and there will be some governance surrounding that from the person who has hired or commissioned them to do it. There are some difficulties if people are just going off on their own and doing it—difficulties for themselves, indeed—and they do not have the protection of an organisation behind them. That is what normally happens.

Andy Smith: The NUJ code of conduct is very clear in stating that investigations should be done by open means wherever possible and that any subterfuge has to be justified in terms of an overarching public interest, so you cannot simply decide to go away and pretend not to be a journalist because you feel that it will be the easiest way to get hold of the information.

Bob Satchwell: It is covered by virtually all codes across the media that you have to have a very good reason for subterfuge. In the new editors' code at IPSO, it is very clear that there is governance on that: at every stage of involvement in an investigation of that kind, notes have to be taken at the time about what the public interest was. It will be recorded and they will be audited on that.

The Chairman: Thank you, all four of you, very much indeed. It was very informative and very useful, and the Committee will be looking carefully at the written evidence that you will be providing us as well.

Rt Hon Theresa May, Home Secretary (QQ 259-282)

Evidence heard in Public Questions 259 - 282

Questions 259-282

Oral Evidence

Taken before the Joint Committee

on Wednesday 13 January 2016

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Lord Hart of Chilton, Lord Henley, and Lord Strasburger

Witness: Rt Hon Theresa May MP, Home Secretary, gave evidence.

Q259 The Chairman: A very warm welcome to you, Home Secretary, for agreeing to give evidence to the Joint Committee this afternoon. You are between the 20th or 25th, I think, of the number of evidence sessions we have had, and, indeed, the last. It has been a fascinating couple of months talking to people from all walks of life, with different views on this subject, but we particularly welcome you, for obvious reasons. It is your Bill, it is one of the biggest Bills that Parliament has ever seen and it is extremely important. We live in dangerous times but we live in times in which it is so important to protect our liberty as well. It is that balance between security and liberty that the Committee is looking at in great detail. So welcome to you.

I am going to start by asking you a question, but if, after I have asked the question, you want to say a few words by way of introduction, the Committee will be more than willing to listen to that. My question is one on process as much as anything else in that the Information Commissioner and the Interception of Communications Commissioner, among others, have suggested that the Bill should be subject to a sunset clause, and if not a sunset clause for the whole Bill, possibly for parts of the Bill. What are your views on that?

Theresa May MP: Thank you very much, Chairman, and may I take this opportunity of thanking the Joint Committee for the work that you have been doing? I recognise from the number of evidence sessions you say you have taken that it has been a very thorough piece of work that this Committee has been doing on, as you say, what is a significant Bill, both in size and in the powers that it holds within it, significant also because of the nature of the threat that we face and the necessity of ensuring that our agencies and police have the powers that they need to keep us safe—with, of course, appropriate safeguards.

In a sense, it is against that background that I would say that from time to time Parliament does put sunset clauses in legislation, often particularly where legislation has been put

through perhaps in an emergency. A recent example in this area was DRIPA—the Data Retention and Investigatory Powers Act—which was put through fairly quickly largely in response to a decision in the European Court. It had a sunset clause enabling us to put into place a longer-term process of developing a piece of legislation that would stand the test of time. That would be my concern about attempting to put a sunset clause in this. We have tried to balance here the need, in a sense, to future-proof the legislation against the need not to produce something so wide-ranging that people feel it is not clear on the powers that are going to be used. RIPA has been in place for 15 years. We would anticipate or expect that this Bill would stand the test of time.

The other aspect to it is that there are certain parts of the Bill that require companies—communication service providers—to take certain actions. Sometimes those actions are ones that require careful planning, and, if you put sunset clauses in, it gives a degree of uncertainty to those very people whom government might be requiring to take certain actions to keep us safe.

The Chairman: A point that has been made, as opposed, for example, to the Prevention of Terrorism Act, which had to be renewed every so often because of the nature of the legislation, is that this Bill is different in the sense that it attempts—and successfully, I suppose—to bring legislation up to date with regard to advancing technology. Would it not be the case, though—and it is inevitable, I suppose—that technology is going to advance even more and that from time to time Parliament would have to have a look at its legislation to deal with that advance in technology?

Theresa May MP: Yes. I am certainly not trying to give the impression that I think this is a Bill that will last for ever and a day. As technology advances, it may be necessary to revisit the powers, the legislative framework and the safeguards that are available, but I do not think advances in technology are going to move according to sunset clauses established by Parliament. The necessity that may come in due course to look again at aspects of the Bill, should it become an Act, would have to be dealt with as and when that arose, rather than artificially putting some deadlines in that might not meet the requirements in relation to the advances in technology.

Dr Andrew Murrison: Home Secretary, do you recognise that there are significant areas of uncertainty in the draft Bill presented to us for consideration at this stage and that some of that uncertainty may very well need to be resolved at a future date? That would mean, naturally, that a sunset clause or a defined period over which this Bill would be in force for review at some future date, perhaps even on a Parliament-by-Parliament basis, might help to deal with issues such as resolution of IP addresses and the definition of ICRs, which remain unclear despite an attempt by the Home Office to improve the definition of ICRs. We sense that, even now, those definitions are unclear—and will be unclear to CSPs especially—and will need to be revisited at some point. In the Bill, if we were able to have some certainty over what sort of period we would be able to do such a thing, it might make for better legislation going forward.

Theresa May MP: I am afraid, Dr Murrison, that I am not sure I recognise completely the impression you have given of the Bill in terms of the degrees of uncertainty that rest within it. You are right that we have introduced a greater degree of clarity in relation to the

definition of internet connection records. On the IP resolution, of course, we did pass legislation in the Counter-Terrorism and Security Act in relation to that. The ICRs provide the final piece of that picture, if you like, in being able to identify people. There are cases today, for example, in paedophile networks, where that identification is not possible because we do not have the ICRs.

There is still a degree to which sometimes people are looking at this and thinking about what was in the draft Communications Data Bill, which was not progressed with by the Coalition Government, and perhaps transposing that into this Bill. We have tried to be very clear on what ICRs are and, indeed, have limited the use of ICRs within this legislation. I know law enforcement has argued perhaps for a wider use of them, but we are proposing that the balance is best met by limiting those within the Bill. With regard to CSPs, we have not had, as far as I am aware, indications from them that in any sense they do not understand what we are talking about in looking at ICRs. We have had numerous meetings with communication service providers as we have been going through the process of determining what should be in the Bill—and the discussions are ongoing—about the technical aspects of the Bill and have had reassurance from the CSPs.

Dr Andrew Murrison: Could you give the Committee your definition of an ICR in terms that might be understandable by a lay person?

Theresa May MP: I will try to do it in an equivalence way in the sense that, when you have somebody who is accessing a particular site or is using the internet for a particular communication, you wish to be able to identify that. You are not trying to find out whether they have looked at certain pages of a website, which is where I think the confusion may arise because of what people felt was in the draft Communications Data Bill. It is simply about that access to a particular site or the use of the internet for a communication.

Q260 **Mr David Hanson:** We have had some compelling evidence about the need for the Bill in relation to the prevention of terrorism, crime and drug abuse and in tracing missing persons from the policing agencies—compelling evidence—but there still remains a body of opinion that worries about the privacy elements of the Bill and what security their own privacy can be given by the state in relation to the access to that information. I think it is really important that you set on the record now for the Committee and the general public what steps you believe need to be taken to retain and secure that privacy, and what associated steps can be taken to minimise risks for the loss of that privacy.

Theresa May MP: If I may, there are three aspects that I would talk about in relation to privacy. You are right, Mr Hanson, to set it out. One of the meetings I had was with representatives of various victims' groups—victims of sexual violence, for example—who were very clear, along with law enforcement, of the importance of the powers in the Bill. The safeguards available for individuals in relation to the powers within the Bill are various. First, there are the authorisation procedures, and in relation to the most intrusive powers, namely interception, we are enhancing the authorisation procedure by introducing the double lock of having the Judicial Commissioner looking at a warrant as well as the Secretary of State. There are also the oversight provisions that are provided at various levels, also by the new Investigatory Powers Commissioner—currently provided by a number of commissioners but, as you will know, to be consolidated in that office—who is looking to make sure that the agencies are using their authorities in the correct way and

that proper processes are being followed. There is the oversight that is provided by Parliament itself through the Intelligence and Security Committee. So there are safeguards in authorisation and in oversight.

Then there are also requirements where data is being retained by companies. There are various requirements in relation to the various Acts that those companies need to abide by, such as the Data Protection Act and the Privacy and Electronic Communications Regulations 2003, which require data to be held by the companies in a secure fashion—so, securely. Of course, we introduce the offence in relation to misuse of data that is being retained by the companies.[6]

Q261 Mr David Hanson: There remains a concern as well, though, that communications data definitions—and Dr Murrison has touched on this—remain relatively vague. For example, Clause 195(1) says, "data includes any information which is not data". What does that mean?

Theresa May MP: I completely understand people raising an eyebrow or two at that particular sentence, which I did when I read it myself. I am happy to look at the wording, but it is an attempt to do something very simple. If you talk about data, a lot of people tend to think only about computer stuff—electronic records. We are saying that when we use the term "data" in the Bill it can cover, for example, paper records as well. It is an attempt to be helpful, which, in its language, it has not been.

Mr David Hanson: In an attempt to be helpful—and I genuinely want to be helpful on this occasion—would it be sensible even for the Home Office perhaps to look at the idea of a prescribed list of the elements that comprise communications data and publish them in a statutory code? Would it be helpful to look at separate definitions of entities and entries for telephone data and internet data? I simply ask that because the type of reassurance that that could give might well help the passage of what, as I said at the start of my contribution, is a compelling case for the Act as it will be.

Theresa May MP: Yes, and I completely understand the aim of your question and the intent behind what you are suggesting. The problem is—and it goes back, in a sense, to the first set of questions that I had and the point that the Chairman himself raised—that we are trying to draft legislation that will operate in what can be quite a fast-moving technological world, where things are developing. The more you try and prescribe in more and more specific definitions, the harder it becomes and the shorter the life of the legislation is likely to be. That is a point that David Anderson has made in relation to this. As I said earlier, it is a balance between trying to ensure that legislation is so drafted that it is clear for people but that it is not so drafted that it means it will only have a very limited life, precisely because definitions will move on and there will be developments.

Mr David Hanson: The fast-moving nature of change is one of the potential worries as well. On a personal basis, I did not use Twitter five years ago; I am using it now. I did not have Facebook three years ago; I have it now. With the changes in life—I do not know what is going to come next—I wonder whether or not, going back to Dr Murrison's point again, the definitions are such that they are full of clarity for now and for the future.

---

[6] This offence is at Clause 8 and is in relation to a person in a public authority unlawfully obtaining communications data, whether retained by a CSP or otherwise. (Witness clarification post-evidence session).

Theresa May MP: That is precisely why we are trying to be technology-neutral in the sort of language that we use within the legislation, precisely so that we can provide for developments that may take place in the future. You raised the issue about entities and events. "Entity" is an individual, a device, an event or a communication between devices, for example. The more you try and list, "by definition, communication only covers these issues", then you have, automatically, potentially limited—

Mr David Hanson: But there is a sort of halfway house between a sunset clause on the Bill and a statutory code that could be issued potentially every two years indicating what is covered by the Bill. Would that be a feasible and possible thing to do to offer the security to those who still have the concerns that I expressed earlier?

Theresa May MP: The only comment I would make—and I hope it follows on from what I have been saying—is that if you have a period of time for which a particular code is in operation, unless you have some very easy ways of changing that, you are going to be bound by it for that period. If something comes up in between, you may find that you are caught unable to use a power in a way that is necessary to keep people safe because of the well-intentioned attempt to try and give greater definition in these matters.

Q262 **Suella Fernandes:** In relation to communications data we have heard evidence from the head of the Metropolitan Police Service Technical Unit, who has said on record that they are struggling to keep apace with technological development, and the use of communications data is integral, in theory, to inquiries into theft, child sexual exploitation, homicide and fraud. What is your opinion on extending the number of purposes for which law enforcement and agencies can obtain communications data—for example, for the purpose of saving life, such as identifying vulnerable individuals in circumstances that may not be considered an emergency?

Theresa May MP: It is important that access to communications data is available in circumstances where it is about saving life. The definition of an emergency will cover a whole range of circumstances where the police will suspect that somebody is in danger and that there is a requirement for them to access this data. That is why I have been comfortable with using that phrase in terms of the emergency. I have tested with my officials certain circumstances where saving a life might arise, and I think in all those that I have looked at it would be covered by the definition of emergency. Almost by definition, if the police or another authority are trying to intervene to save a life, that is an emergency circumstance.

Suella Fernandes: The case that comes to mind is that of a missing person where there is a suspicion or information that someone has gone missing and they are a vulnerable person, but in the current regime there is a difficulty in defining that necessarily as an emergency.

Theresa May MP: There are a lot of developments taking place in how police deal with MISPERS—missing person cases—but if there is a suspicion and a concern that there is a genuine threat to life for that individual, I would expect that to be able to be covered by the use of the term "emergency".

Suella Fernandes: What is your view on extending the purposes to cover those crimes that are not "serious crimes" but where it is still necessary and proportionate to obtain that data?

Theresa May MP: It is important for law enforcement to be able to access communications data in these circumstances. There is a formal definition of serious crime, but there will be other crimes—for example, maybe harassment online—where access to data is important to identify perpetrators and deal with that crime but which does not necessarily fall into the formal definition of a serious crime. It is for that reason that it is important for the police to be able to have access to communications data in other circumstances.

Q263 **Shabana Mahmood:** Home Secretary, could I take you back to the issue about internet connection records and the definition, following on from your exchange with my colleague Dr Murrison? We have only recently had the Home Office's submission with the additional information. We have not had an opportunity to put that to all the numerous witnesses who have given evidence or might have wanted to give us written evidence on those. Our very preliminary advice or initial soundings are that the issue is not that there is no understanding about where you are trying to get to. In fact, you said in your answer that there is understanding of what you are talking about and your dream scenario of the information you are trying to get to. The problem is whether it is technically feasible, given the way that the internet works. Our understanding at the moment is that there is no real agreement or understanding of the technical path to get you to the kind of data that you want. What is it that makes you so confident in the answer you gave earlier that that technical path to your best scenario for internet connection records is going to be found and met by all the CSPs?

Theresa May MP: The confidence we have comes from the discussions that we have been having with CSPs. As I indicated earlier, we have had numerous discussions with them about how access to ICRs may be achieved. Chairman, in my answer earlier to Mr Hanson and to Dr Murrison, I was not trying to suggest that there would be no way in which we would be trying to get some greater clarity of definition perhaps through codes of practice. There was a specific issue around timetabling and so forth. We are talking to the CSPs, and the discussions we have had with them have been about some of these technical issues about access. There are different ways in which different providers approach the way they operate, but we are confident from those discussions that it will be technically feasible for us to ensure that there is access to the information that is necessary.

Shabana Mahmood: Even if each of them goes about it slightly differently, you are confident that the end product will be basically the same.

Theresa May MP: Yes; we are confident that we will be able to have the access that is necessary.

Q264 **Shabana Mahmood:** A lot of my constituents wrote to me about this description of internet connection records being like an itemised telephone phone bill. Other people have said—and lots of Members of Parliament can relate to the sorts of communications we have had from our constituents—that this is a very unhelpful, misleading characterisation of what an internet connection record will look like. Would you agree that that is probably not helpful and we should avoid it?

Theresa May MP: It is, again, another attempt to be helpful in describing. The point of the comparison is to say that at the moment law enforcement and agencies have access to data in relation to telephony, which enables them to identify, if somebody has gone missing, with whom they have been in contact prior to going missing. As people move from telephony to communications on the internet, the use of apps and so forth, it is necessary to take that forward to be able to access similar information in relation to the use of the internet. I would say it is not inaccurate and it was a genuine attempt to try to draw out for people a comparison as to what was available to the law enforcement agencies now—why there is now a problem—because people communicate in different ways, and how that will be dealt with in the future. It is about communications from one device to another.

Q265 **Shabana Mahmood:** I suppose in a way your answer helpfully illustrates the difficulties that we are all grappling with when it comes to how to accurately describe exactly what is going on.

Can I move on to the experience of Denmark? We have had a fair amount of evidence on how a similar regime worked in Denmark, which was then ultimately scrapped. There were some very significant differences between what happened in Denmark and what you are proposing here, in particular the coverage of the scheme, as it were, in Denmark; their scheme did not cover access to the internet by smartphones for various technical reasons, but there were similarities around the desire to have IP address resolution and so on. They found in Denmark that they just collected a huge amount of data of limited utility. It was not particularly effective in helping the police to do their job. What is your view of what happened in Denmark, and why would you say that what you are proposing here is significantly different and therefore more likely to be useful?

Theresa May MP: As you might imagine, we have been talking to the Danes about their experience. There are a number of ways in which it is different. One of them is in relation to how information is due to be collected. I would best describe it—as it was described to me—that part of this is about at what point on the network you are accessing the information. We will be accessing it at a different point from the point at which the Danes were accessing it. They were getting a lot of peripheral information that did not enable them to link accounts to users, as I understand it. Another element is what we have already done in relation to IP address resolution through the Counter-Terrorism and Security Act. When you put these together, it gives us that greater capability.

There are some other differences in relation to costs, for example, in the Danish system. As I understand it, the costs were borne largely by the CSPs. We have an arrangement for providing for cost recovery here in the UK. There are a number of differences, but, in talking about the point at the network, it is trying to do it in a simplified way, which shows that there is a technical difference in the way we are doing it.

Shabana Mahmood: I understand the technical point you are making. One thing we have had quite a bit of evidence on is the amount of data you will be collecting and what it will ultimately tell you. One of the problems we have had some evidence on is about constant connection and that smartphones will almost always be connected to the internet by all the different apps. Therefore, the information you are collecting is only going to tell you the point at which the app was activated and not anything else because it is constantly connected to the internet. Do you see a danger that, in the end, you will just collect a vast amount of data that is of

limited utility to the police, if, for example, in a missing persons case all they can tell is basically when somebody downloaded an app on their phone and not very much more than that?

Theresa May MP: Certainly in relation to this issue of volume of data, which was something that was raised in the Danish example, they did find that they had a large volume of data. We will have a more targeted approach, which we believe will reduce that overall volume of data recorded and reduce the risk that connections are missed. I was hesitating to say, Chairman, that I am reliably informed that the Danish implementation was based around sampling every 500th packet rather than recording individual internet connections or sessions, which is what we propose to do. I do not think there is going to be that volume of data in the much more targeted approach that we will take.

Q266 Stuart C McDonald: I have a couple of questions on internet connections, if I may, Home Secretary. Correct me if I am wrong—it has been a few weeks since I have read it—but the operational case for internet connection records is about 25 pages long. As far as I can see, it does not contain any mention of terrorism. Instead it focuses on fraud and child sexual exploitation. Is there a particular reason for there being no mention of terrorism in that operational case?

Theresa May MP: No. The case in relation to communications data and internet connection records has been one on which particularly the law enforcement agencies have given some examples of ways in which they can show the importance of this. That is one reason why we have tended to focus on that, and we can give those sorts of case examples in relation to that, but this is a capability that would be available to law enforcement and indeed to the agencies. I do not think there was a deliberate attempt to exclude terrorism, but, in looking at the operational case, sometimes it is easier to explain some of the cases that relate to issues like paedophiles and child exploitation.

Stuart C McDonald: Following on from what Ms Mahmood has been saying, there is one set of arguments about the utility of these internet connection records. For example, as you explained it earlier, an internet connection record would explain that I had contacted the Facebook website but it would not tell me who I had been communicating with or when and so on; so there are questions about the utility of that information. On the other hand, if you were to put together 12 months of my internet connection records, you would find out a hell of a lot about me, and I will not go into what you might find out about me. You can see why that would be quite invasive on the one hand and yet on the other hand there is this question about utility. How would you respond to those concerns?

Theresa May MP: As I indicated in response to an earlier question, the intention of this is not to find, in some sense, people's web-browsing history, which I think was one of the issues that was raised in relation to the Communications Data Bill, looking at exactly what everybody was looking at all the time and the pages behind the first web page that they went to and so forth. As you will have seen in this legislation, we have limited the purposes for which access to internet connection records can be used. As I said earlier, law enforcement, I know, have indicated that they would prefer to see fewer limits. They think they can put a case for extending that. We have looked at the balance of the concerns that people have had about privacy against utility and that is why we have come up with that specifically limited set of access arrangements.

Stuart C McDonald: The response to that might be that, if you are going to start gathering this data and it is quite invasive, you might as well use it for a broader range of purposes. Going beyond that, you have recognised that the operational case concerns examples from law enforcement, in particular, but we then get to the stage where it is a struggle to see why finding out that a missing person has been using Facebook cannot be done by other means—simply by speaking to the person's friends or family or by going on Facebook directly. Can we get more examples of the utility of these internet connection records that will help to persuade us that this invasiveness and collection of data will be worthwhile and worth the dangers that come with it?

> ***Theresa May MP***: I note the point that you made earlier about the potential arguments for increasing the purposes for which the information is collected. One of the benefits of the joint scrutiny committee is that it is a Committee that can challenge and look at those issues and make recommendations. If you are asking whether we can provide some extra examples and exemplifications that could show the utility of internet connection records, I am very happy to do that for the Committee. You mentioned a number of ways in which police would gain other information in relation to a missing person. Of course, in any investigation that the police undertake, whether it is for a missing person or whether it is a murder investigation, they look at a variety of forms of evidence in order to build the picture that they need to have to solve the crime or save the life. What they are saying—and what I am saying—is that as part of that, against the background of appropriate restrictions, oversight and safeguards, it is important that they are able to have access to this part of the picture as well.

Victoria Atkins: This follows on, Home Secretary, from Mr McDonald's question about the operational case, particularly with regard to terrorism. Yesterday Assistant Commissioner Mark Rowley, who leads the counterterrorism operation nationally, gave evidence to the Home Affairs Select Committee that communications data is used in 100% of terrorist investigations and prosecutions. Does that accord with your knowledge as Home Secretary?

> ***Theresa May MP***: Yes, it does. It is also my understanding that it is used in something like 95% of serious organised crime cases—often, evidentially in prosecution.[7]

Victoria Atkins: So those percentages are very much in mind when considering the civil liberty arguments that many witnesses have given to this Committee.

> ***Theresa May MP***: Yes, indeed. I recognise that, because of the nature of the powers we are talking about in this Bill, it is always necessary to look at the utility argument and at the privacy argument. Communications data is an important part of the process that law enforcement, in particular, will go through when looking at these cases—when dealing with terrorist cases, as Assistant Commissioner Rowley has said, but in serious and organised crime cases as well. That is why we think that, in the internet age, we need to have this extension in relation to internet connection records. What is important—and what we are doing in this Bill—is the oversight arrangements. It is important that the legislative framework is right, the oversight arrangements are right and the authorities and safeguards

[7] 95% of prosecutions handled by the Serious and Organised Crime Division of the Crown Prosecution Service (Witness clarification post-evidence session).

are right, so that people can have confidence in the system, while knowing that, if this information was necessary in order to keep people safe, it would be available.

Q267 Mr David Hanson: I turn to data retention. The Bill proposes storing internet connection records for 12 months. I have three simple questions. How much will it cost, when will the capability be available, and who will pay?

Theresa May MP: We have provided some indicative figures in relation to—

Mr David Hanson: You have. It is £247 million in the Bill.[8]

Theresa May MP: Yes. As I said, we have provided some indicative figures. Obviously we are still in discussion with individual CSPs about the ways in which these capabilities would be provided. We provide reasonable cost recovery. That has been a long-standing policy of the UK Government, where we are requiring companies to do things in order to have this sort of access.

Mr David Hanson: At one oral session on 14 December, we heard evidence from Vodafone, O2, EE and the regulatory engagement officer from 3. That is just four providers. Basically, they said that they alone could spend the £247 million[9] and that they do not have the capacity currently to store the records required by the Home Office. The challenge to you from the Committee is, can you justify to us today—or at some point—that there is sufficient resource to meet the requirements that have been placed on providers and that they have the capacity to put this into practice in a reasonably short amount of time? Can you also indicate what the repayments will be? For example, Adrian Gorham of O2 said, "It is going to be huge". Mr Jonathan Grayling of EE said, "If there is a cost recovery model that places a cap on cost", it will be very difficult for them. These are important issues. Whatever our objectives, can you deliver it, for the budget that you have, in the timescale that you want, to the satisfaction of the providers?

Theresa May MP: Precisely one of the reasons why we are having such detailed discussions with providers is that we have been going through this and talking to them about the sorts of ways in which this would be provided, about the technical feasibility of it—that is why we are confident of it—and about the sums of money that would be necessary. If the Committee would like some further indications in relation to those matters of technical feasibility and cost, I would be happy to provide them. We have not just been sitting there as the Home Office saying, "We think this is a good idea. Let us pluck a figure out of thin air, put it into the Bill and the explanations, and just hope and pray, on a wing and a prayer, that people can do it". We are talking to them in detail about how this would be provided, and they have been responsive. I can say that, because I myself have had a number of meetings with CSPs at which they have shown me that responsiveness on this matter.

Mr David Hanson: I think I speak for the Committee when I say that we have picked up a slight nervousness among them that they can deliver on time and on budget and have cost

[8] The ICR provisions in the Bill have a cost estimation of £174.2 million, discounted, over ten years. The overall costs of the CD provisions are £187.1 million discounted, over ten years. The £247 million cost in the Bill's impact assessment includes the cost of the internet connection record provisions as well as the costs for the request filter and changes to the oversight regime. (Witness clarification post-evidence session).
[9] *Ibid*

recuperation. It is important that there is clarity from the Home Office that what you are requesting can be delivered.

Theresa May MP: I believe that the discussions that we have had show both the technical feasibility of, and the ability to deliver on, this capability, but if the Committee would like some further written evidence from the Home Office on that, we can certainly provide that.

The Chairman: That would be very useful. Mr Hanson has put his finger on a problem that came up during the various sessions with communications service providers. They were troubled about costs and whether they had the capacity physically to store the data, including buildings. You say that you are in continuous discussion with those companies. It would be very useful if we could have some detail. Thank you very much.

Mr David Hanson: The second issue on data retention that has been raised with us is the question of a security risk. Balanced against that, we recognise that large banks, Tesco and Google have massive amounts of personal data on individual citizens that is kept perfectly secure. However, I would welcome your assessment of how you anticipate key data on internet connection records being kept secure by third parties from, for example, cyberattack or internal leaks from individuals within that system. Again, that goes crucially to the centre of the concerns that have been expressed about what is a very compelling argument for that information to be kept.

Theresa May MP: Indeed. I fully accept the importance of the issue of security for people in relation to the data that will be kept. We make clear—and it will be clear in the code of practice—the importance of ensuring that there is that degree of security. As I indicated earlier, there are already safeguards in place in relation to data security. There is the requirement to comply with the Data Protection Act 1998 and the Privacy and Electronic Communications Regulations 2003. That requirement includes ensuring that there is appropriate security of data. Communications service providers will also be subject to data retention notices, which must comply with the requirements in the Data Retention Regulations 2014, the data retention code of practice and any specific security requirements that may be in the notices themselves. All those requirements will be replicated in the Bill, the codes of practice and the notices that are issued to the companies, so there is a requirement on the CSPs to maintain an appropriate degree of security. Of course, the Bill provides effective oversight by the Information Commissioner, which can ensure that data is held securely.

Mr David Hanson: A particular concern has been raised with us about what we will call third-party data, which is information that businesses would not normally keep for their own business purposes but that it is now suggested they keep. I wonder how the Home Office will assure CSPs that they are not required to retain third-party data. Can we get some clarity around that particular issue?

Theresa May MP: We have made it very clear that we will not require CSPs to retain third-party data. When I talk about third-party data, I am talking about services that run across their network but that they themselves do not provide. This is a key difference between this legislation and the draft Communications Data Bill of 2012, in which we proposed that third-party data should be retained by CSPs. It has always been possible for public

authorities to acquire third-party data, where it is held by CSPs for business purposes or where they can extract it on a forward-looking basis. That can be beneficial in investigations, but they are not obliged to comply with the requirement to extract third-party data where it is not reasonably practical for them to do so.[10] The concern that the companies raised specifically with me was the suggestion that they should have to hold data that was going across their networks and related to services that they did not themselves provide. We are not requiring them to keep that data.

Mr David Hanson: I have one final question. How will the Home Office enforce data retention by those providers that are offshore from the United Kingdom?

Theresa May MP: There are certain aspects of this legislation where we are looking at extraterritoriality. However, there are requirements that we will issue. As you know, data retention notices will be issued to communications service providers in relation to the requirement for them to hold data in a way that enables that to be accessible.

Suella Fernandes: Following on from the point raised by Mr Hanson about cost and the estimates that have been provided by the Home Office, could you set out and explain to what extent the Home Office has engaged with the ISP Association and individual CSPs, and whether or not the estimates are born out of those discussions?

Theresa May MP: Yes. Some interaction with communications service providers has been done on a collective basis, but there have also been discussions with individual communications service providers. There is a recognition that, for individual providers, there may be some aspects of their business that they would not necessarily wish to discuss in front of others. It is from those discussions that we have the confidence that we have in relation to the ability to provide this access to internet communication records.

Suella Fernandes: Traditionally, large CSPs will incur very different costs and burdens to small CSPs, so recovery is granted on a case-by-case basis. Is that right?

Theresa May MP: Yes. We will look very carefully at those CSPs on which the requirements are placed. It would be helpful if notices could be served on some small CSPs that have a very specific niche in the market or specific geographical coverage, but obviously we will look at the necessity and proportionality of that on a case-by-case basis.

Q268 **Matt Warman:** My question is a follow-up to that, in many senses. Obviously we would expect a retention notice to be served on the largest providers and some specific smaller ones, but some of the smaller ones have expressed uncertainty about whether the expectation is that they should stand ready to be served with such a notice or whether there is a standard that they can reasonably expect to escape, if they are quite small. I do not expect you to say that anything below a certain size will never be touched, but will there be a deterrent effect? Will there be any clarity on that?

Theresa May MP: There is not an intention to describe a CSP that would never be served with a data retention notice, precisely because of the point that I made in response to Ms

[10] Third party data is data which is about services a CSP does not provide, which they do not need to process to deliver the service and which they do not keep for business purposes. (Witness clarification post-evidence session).

Fernandes—that it may be that a smaller CSP covers a particular geographical area or a particular niche in the market. We would not look to describe a CSP on which a data retention notice could be served and a CSP on which a data retention notice could not be served. We have to have that degree of flexibility. Wherever the intention is to serve a notice, of course, there is a discussion with that company about its ability, the requirements that might be needed and the technical feasibility of those requirements. We are required to look at the technical feasibility, the costs and any other impact on the CSP. Of course, we are introducing the right of appeal for the CSP, when a notice is served on it.

Q269 **Matt Warman:** Is it your understanding that a CSP might include things such as people running a wi-fi network in a coffee shop? That is the example that is often used. Do you understand that those would definitely be included, potentially? Could you talk a little about the justification for those sorts of retention notices?

Theresa May MP: Yes. That is left open—and rightly so. If you look at how people are conducting their business, their interactions and their communications today, they are doing that on the move and in a whole variety of settings. It may very well be that there are circumstances where it is appropriate to have that discussion and, potentially, to ask for information to be retained. It is about having that flexibility.

Matt Warman: Might those private networks include university networks or company networks, for instance?

Theresa May MP: I do not think that it would be right for us to exclude any particular type of network, because of the way in which people conduct their business and their interactions these days. However, for any individual decision, there is an onus on the Home Office to look at the necessity and proportionality of that, the technical feasibility of that, what the costs would be and what the impact on that particular CSP or network would be.

Lord Butler of Brockwell: Will the fact that you are having discussions with CSPs or ISPs—and, indeed, the serving of notices on them—be a confidential matter?

Theresa May MP: The serving of notices on them would be a confidential matter. We would not look to make that a public matter. For obvious reasons, when one is looking at the reasons why we should have access to this data and, therefore, require its retention, I would not want to suggest that there are particular CSPs that people could migrate to purely because a retention notice has not been issued on them.

Lord Butler of Brockwell: That is what I had in mind. Would it be possible to maintain that confidentiality if, for example, you were going to bring proceedings against them? Would they be immune from applications under the Freedom of Information Act, if you were asked on which providers notices had been served?

Theresa May MP: I will check the issue on the Freedom of Information Act, if I may. Obviously there are some elements of exclusion under the Freedom of Information Act in relation to national security matters, in particular, as well as some matters relating to law enforcement. I am very happy to write to the Committee with more specifics on that point.

Dr Andrew Murrison: Can I ask a little more about so-called coffee shop ISPs? Most of us would be comfortable with the process affecting CSPs, since they tend to be larger operators, but potentially there is cause for some very small operators to feel distinctly threatened by all of this—and, possibly, to be targeted by the process. Can you be absolutely clear that the costs that will bear on those small operators will not be disproportionate?

Theresa May MP: As I indicated earlier, we are operating on the basis of cost recovery, in relation to the Government providing some funding in these areas. In looking at and having the discussion with a particular provider in relation to retention of this data, the issues of the impact on that provider—the costs—would be taken into consideration. Of course, that would be balanced against what the expectation would be with regard to the necessity of access to data. Those sorts of considerations would be entered into.

Q270 **Dr Andrew Murrison:** Can I press you on the vexed issue of encryption? Most of us who use the internet would probably regard end-to-end encryption as a very good thing. Indeed, many CSPs use it as part of their business model. In general, security is promoted by encryption, yet the Bill talks about "removing electronic protection". We have heard terms such as "establishing a back door" for the agencies to access information. Clearly, there is a threat that businesses that wish to conduct their operations with a degree of privacy may note the relative prurience of the British system, as articulated in the Bill, and choose to move their businesses outside, if they cannot guarantee to their customers the sort of privacy that other Administrations can. Could you give us some indication of what you mean by "removing electronic protection" and what the implications of that are for end-to-end encryption? Could you also outline any worries that you may have about the apparent intention of this Bill to end the degree of security guarantee that applies in the UK at the moment?

Theresa May MP: I am grateful for the opportunity to provide a degree of clarity, I hope, around the issue of encryption and what we are proposing on that in the Bill, because there has been some commentary that has not accurately reflected what we are intending to do in the Bill. As a Government, we believe that encryption is important. It is important that data can be kept safe and secure. We are not proposing in the Bill to make any changes in relation to the issue of encryption and the legal position around that. The current legal position in respect of encryption will be repeated in the legislation of the Bill. The only difference will be that the current legal position is set out in secondary legislation and it will now be in the Bill. We say that, where we are lawfully serving a warrant on a provider so that they are required to provide certain information to the authorities, and that warrant has gone through the proper authorisation process and is entirely lawful, the company should take reasonable steps to ensure that it is able to comply with the warrant that has been served on it. That is the position today, and it will be the position tomorrow under the legislation.

Dr Andrew Murrison: CSPs will then say, "Because we have end-to-end encryption, we are unable to help you with that". Can I press you a little more on what removing electronic protection would mean in practice?

Theresa May MP: What we say to companies today and will say to companies under this legislation is that, when a warrant is lawfully served on them, there is an expectation that they will be able to take reasonable steps to ensure that they can comply with that

warrant—i.e. that they can provide the information that has been requested under that lawful warrant in a form that is legible for the authorities.

Dr Andrew Murrison: So you are not looking to them to provide a back door for the agencies or a key, as it were.

Theresa May MP: No. We are not saying to them that the Government want keys to their encryption—no, absolutely not.

The Chairman: You want translation, in a sense, so that whatever information the warrant demands is readable by those who need to read it.

Theresa May MP: Yes.

The Chairman: But the company's encryption facilities would be safeguarded.

Theresa May MP: Yes. The Government do not need to know what the encryption is or to know the key to the encryption. It is exactly as you say, Chairman. If there is a lawful warrant requesting certain information, it is about that information being readable.

Q271 Lord Strasburger: Good afternoon, Home Secretary.

Theresa May MP: Good afternoon.

Lord Strasburger: Can we move to the vexed question of the many bulk powers that are in the draft Bill? Those involve large-scale state hacking, surveillance and copying of data, which, to a very large extent, belongs to people who have no involvement whatsoever in crime. We have heard from the security and intelligence agencies and a few other witnesses that those powers are useful and necessary, but a much larger number of witnesses and written submissions—by no means only from civil society groups—have argued strongly that these powers are overly intrusive, disproportionate and so are illegal under EU law. My first two questions are: can bulk powers ever be deemed proportionate, and on what basis does the Home Office believe that these mass surveillance powers will be seen as legal in the context of recent European court decisions?

Theresa May MP: I am tempted to say, Lord Strasburger, that, by definition, my answer to your first question has to be yes, precisely because there are powers that exist today in relation to bulk matters, and those will be within the legislation. It is the case that there are occasions when this is proportionate. Of course, we have seen challenges in the European courts in relation to the question of data retention, which led to the Data Retention and Investigatory Powers Act 2014. In relation to those matters, we believe that what we have put in our DRIPA legislation and what we will bring into this legislation meets the requirement. I do not think it is clear that the European Court of Justice judgment intended to impose minimum standards. We believe that our current regime is compliant with the requirements of EU law and that the regime that we are proposing and the legislation that we are bringing forward are similarly compliant with EU law. As you know, there has been a test case in relation to DRIPA in the UK courts. The Court of Appeal also agreed that it was not clear that the European Court of Justice intended to impose minimum standards in relation to these matters and has decided to refer questions about

the interpretation that has been taken of the case with the ECJ—the Digital Rights Ireland case—to the European Court.

Lord Strasburger: I guess that time will tell. There is a risk that the Bill, if it becomes an Act, will be overtaken by something that happens in the courts, but time will tell.

We have also heard from many witnesses that bulk powers are operationally counterproductive, because agency analysts are being blinded by the huge volumes of data that are being collected. We have also heard that the problem will get much worse, because in 10 years' time the massive quantities of data will have increased by a further factor of 1,000 or more. For almost every recent terrorist attack in the West, one or more of the perpetrators was previously known to the intelligence agencies and was somewhere in their database, yet they were not picked up as an imminent threat by the analysts, who are drowning in data.

We heard last week from a former NSA technical director that the very expensive approach of the NSA and GCHQ—namely collecting all the data all the time—causes the agencies to miss opportunities to prevent attacks. That means, we were told, that avoidable deaths will occur in the future and that 9/11, 7/7 and both Paris attacks could have been prevented. He and others argue for a much more targeted collection of information, which works because analysts see manageable quantities of data that still includes the bad actors they are looking for.

My question is, what do you think of making it more likely that we will find the needles by shrinking the haystack, with smart, targeted collection?

Theresa May MP: May I pick up on a number of the comments that you made in your question, Lord Strasburger? First, I must challenge your reference to the UK authorities "collecting all the data all the time". We do not collect all the data all the time. I wish to be very clear with this Committee that that would be a misdescription and a misrepresentation of the action of the UK authorities.

I would also remark on your references to a number of terrorist attacks that have taken place and the comment that you say somebody made to the Committee that those could have been prevented. The inquest on 7/7 that took place under Lady Justice Hallett was very clear in its findings, which were of a different nature from what you have suggested in relation to that.

To put a very simple point, which is a point that a former Home Secretary—not, as it happens, from my party—used to make, "You cannot look for the needle in the haystack unless you have got the haystack". In some cases, you need to be able to access this data to identify it. There are a variety of ways in which the agencies are careful and look to target how they deal with data. However, if the suggestion is that you cannot collect any bulk data or have access to any bulk datasets whatsoever, you will miss the opportunity. I do not see that that helps you to deal with the circumstances and issues that you are raising.

Lord Strasburger: You and I have discussed haystacks in the past. The evidence we heard last week was that the haystack now is so big that although we know that data about the perpetrators of those texts that we have mentioned was in there—we know that is the case—it was not picked up and identified as a threat by the analysts. The suggestion from Mr Binney

last week, who is not an inconsequential witness being the technical director at the NSA, was that the reason they were missed was because the analysts who were supposed to spot them were drowning in too much data that was nothing to do with what they were looking for. I only report to you what we were told last week.

Theresa May MP: Yes; I was looking through that. I knew I had the reference to what he said here. First of all, as I indicate, it would be wrong to give the impression that we are collecting all of the data all of the time. Once again, I want to be very clear about that. But bulk capabilities are important because, if you are going to be able to investigate a target, you need to be able to acquire the communications in the first place. When the target is overseas, bulk interception is one of the key means, and indeed may be the only means, by which it is possible to obtain communications. It is not the case that it is always used in an untargeted way. Once again, I would challenge that in relation to these issues.

When particular incidents have taken place, of course we look at the systems that are in place to ensure that we can make the way we operate as effective as possible. There is a very fundamental reason for being able to have access to this information and being able to deal with this information. It is about keeping people safe and secure.

Lord Strasburger: Finally, on mass surveillance, Home Secretary, we have seen an operational case for internet connection records but we have not as yet seen one for bulk acquisition of communications data, bulk equipment interference, bulk interception and bulk personal datasets. These powers have been used for some time, despite not being revealed until 2015 and never having been approved by Parliament. In a supplementary paper just a few days ago, David Anderson warned, "If an evidence-based public defence of these powers is not attempted, the argument may yet be won at the European level by those who assert the powers to be either useless or more sinister in their operation than is in fact the case". My question is: when will the missing operational cases be published?

Theresa May MP: I am sorry, Lord Strasburger, but again I want to challenge one of the phrases you used in your question to me. You indicated that what we were doing was mass surveillance. You described it as mass surveillance. The UK does not undertake mass surveillance. We have not undertaken, and we do not undertake, mass surveillance. That is not what the Investigatory Powers Bill is about.

You referred to bulk equipment interference. This is important. There will be cases where it is necessary to use that in order to be able to keep pace with those who want to do us harm, where it is not possible to disrupt and intervene on activities through interception, for example. If you are asking me to write to the Committee to give a further explanation of why I think the bulk powers are necessary, of course, Chairman, I can do that, but I would wish to be very clear that mass surveillance is not what we are talking about.

Lord Strasburger: I accept you are very clear about that. I want to be very clear about the fact that these four powers have never been before Parliament—ever. I did a search of Hansard. If you look for "equipment interference" or all the other terms I have just mentioned, they are not mentioned until 2015, and one of them just two months ago by you. It is rather important, now that they are coming before Parliament for the first time, that there is a proper justification and explanation of what is involved, what the liberty and financial costs are and so on. We have had it for internet connection records, but for some reason we have not had

it for the other four. I am just asking that the Home Office publishes an operational case for it. Mr Anderson says that it is very much in the Government's interest to do so, because without those operational cases the Government are going to run into a lot of trouble in the European courts.

Theresa May MP: One of the aims we have had in relation to the Bill, which I have been very clear about on the Floor of the House, has been to give a greater degree of transparency and clarity to people of the powers to which the authorities do have access—

Lord Strasburger: I congratulate you for that.

Theresa May MP: —and the legislative framework for that. One of the purposes of having the processes of scrutiny that we have had on the Bill is precisely for these issues to be looked at, which is why, as I indicated earlier, I am grateful for the work of this joint scrutiny committee. There are a number of reasons why it is important to have these various bulk powers. I have given a number of references here, but I am very happy to put that in writing to the Committee.

Q272 **Lord Strasburger:** Turning to bulk personal datasets, the lack of clarity about them has been a concern for many witnesses and Committee members. We understand that there are databases that exist in the public and private sectors and that each contains personal information about potentially millions of innocent citizens. We also understand that the security intelligence agencies have for some time been getting copies of this data, either with or without the owner's permission, and once again without the explicit approval of Parliament for them to do so. Some witnesses have told us that these datasets have been medical records, bank account data and other highly personal information. In order to establish the truth about bulk personal datasets, the Committee has asked the Home Office many times for a list of them, which has been refused on every occasion. My question is: how can the Committee form a view on the appropriateness of the secret ingestion of bulk personal datasets without having any idea what they are?

Theresa May MP: I understand, Chairman, that the Security Minister has written to the Committee today on this matter, explaining why it is the case that we do not list out the various bulk personal datasets to which access is provided. I am happy to give you examples. I think everybody would accept that a list of people with a firearms licence would be very useful if you are looking at people who are of particular concern to law enforcement and the agencies, to be able to see who has access to firearms. The letter that has been sent today—and I fully recognise that it may not have been possible for members of the Committee to have looked at it yet—sets out why it is the case that we do not list out every single personal dataset that may be accessed. I think it is important for us to do so, and we are very clear in a number of areas that it is important for us to retain that degree of flexibility precisely because of the sort of people that we are dealing with.

Lord Strasburger: It is not possible to exclude certain datasets like medical records.

Theresa May MP: No. As soon as you start excluding certain datasets, that gives messages to those who would seek to do us harm about the way in which the authorities operate.

The Chairman: It was an issue that exercised the mind, for example, of the Information Commissioner when we questioned him last week. Three other members of the Committee want to come in on these issues. I would ask them to be reasonably concise because we have to move on to authorisation. Dr Murrison, Ms Atkins and Ms Fernandes, please be concise.

Dr Andrew Murrison: I will be brief. Home Secretary, I want to press you on this issue of the nature of the datasets. It seems to me that there is a continuum at one end of the sort that the Home Office has very helpfully told us they would be focused on. You have mentioned firearms certificates, passport applications, electoral roll material and telephone directory stuff. Some of it is in the public domain already, of course, which is very innocuous and which I suspect the public would have absolutely no difficulty with at all. At the other end, there is stuff that may not actually be public record at all, either explicit or private. I am thinking of things like medical records—which are increasingly important as we move towards electronic medical records—clinic attendance and bank accounts. Those are highly sensitive things. What would be reasonable without being specific, and I accept the reasons for not being specific, is for you to say where on that spectrum you would expect attention to be focused and cut off. It is important that people do know whether in fact the intention of this legislation is to tap into very personal material of the sort I have described at the far end of the spectrum, or whether you feel that your attentions will be focused and sighted specifically in this Bill or through codes of practice. It is important that we have some better sense of where this is going to fall, other than from what you have already provided us with.

> ***Theresa May MP***: If I may, Dr Murrison, I would approach the issue from a slightly different angle. What we are doing in the Bill is not listing out the datasets but providing for a greater degree of safeguard in relation to the acquisition of datasets through the warrantry process with the double-lock authorisation on the warrantry process. The fact that these datasets are available and are accessed is something that is looked at in the current oversight arrangements by the relevant commissioners. They have recognised that this is an important capability. It is also the case that the Intelligence and Security Committee can scrutinise any classified elements in relation to this to provide this Committee with greater reassurance, if that is helpful. As I say, the important thing is to know that these are being accessed in accordance with safeguards and authorisation processes that ensure that double lock, which will be the case in terms of warrants for bulk personal datasets, and which ensure their necessity and proportionality.

Dr Andrew Murrison: What would at least be helpful is if you could say whether or not the four examples I have just given would be typical of the sort of thing you would expect to be collected through this process, as opposed to simply being examples. You will appreciate the clear difference between the two.

> ***Theresa May MP***: I do, but, as I have indicated in response to Lord Strasburger and has been indicated by the Security Minister in the response to the letter, which I recognise that not all members of the Committee may have had an opportunity to see, we do not feel it is right to go down the route of giving information about the sort of datasets that would be acquired and the sort of datasets that would not be acquired. You are asking me, I think, what is, in a sense, a less specific version of the question that Lord Strasburger asked me, which is why I am giving you the same answer. The important thing in relation to the privacy angles and in relation to ensuring that the authorities are only doing what is necessary and

proportionate here is the fact that there will be a warrantry process that will have that double-lock authorisation in it. There will be an oversight process that provides that safeguard for people.

Victoria Atkins: Lord Chairman, this is really a point to clarify the evidence that was given last week by Mr Binney. Lord Strasburger has not mentioned it, but I think it is important that it is on the record given that this is being televised and there are members of the Committee who were not in that evidence session. Mr Binney conceded that he was last cleared for security with the NSA 15 years ago, and his evidence at the end was that he was accusing all the law enforcement officers and security service officers of being wrong in their evidence to this Committee, and possibly misleading this Committee. I think it is important to put that in context when Lord Strasburger cites Mr Binney's evidence. It will be a matter for the Committee in due course to decide the weight to attribute to Mr Binney's evidence.

Suella Fernandes: I have two simple questions. Home Secretary, in the context of the access to bulk data, do private companies like large retailers, charities and other technological companies have bulk access to data, to your knowledge?

Theresa May MP: There are bulk personal datasets that are in the public domain and to which I am sure organisations other than Government have access.

Suella Fernandes: It is part of our digital society, is it not? Lastly, bulk access differs from bulk use of data. What safeguards and limits are in place on the use of bulk data in this regime?

Theresa May MP: I am grateful. Obviously, we talk about various aspects of bulk data and we have just been talking particularly about bulk personal datasets. We have talked about the bulk powers. There are provisions in this Bill, as I have indicated in relation to bulk personal datasets, that introduce an authorisation process that I hope would provide greater safeguards and therefore give greater reassurance to people in relation to how it is possible to access some of these bulk datasets.

Suella Fernandes: Does this Bill represent a codification and clarification of practice, in your opinion?

Theresa May MP: What we have tried to do in this Bill is to be transparent and clear about the powers that are available to the authorities, and crucially to bring powers into one place, into one piece of legislation. One of the comments that was made in the general debate that we had on this matter in the House of Commons was that there was a concern that the current legislation was in different places. We have brought the legislation together and aimed to be transparent and clear so that people can see the sort of powers that the authorities have and are able to use but they can also see the safeguards that are available to them. I think this is world-leading legislation precisely because of that balance that it creates.

The Chairman: Thank you very much. We now move on to the very important area of authorisation with Lord Hart.

Q273 Lord Hart of Chilton: Home Secretary, this is a question about the powers of the Judicial Commissioner in authorising the various issues given for authorisation under the Bill.

Some have said that the powers of the judge are too narrow and are really no more than process checks. Others, including David Pannick, have said that the judges applying a judicial review test must themselves consider the merits and decide whether the measure is indeed necessary and proportionate. Your department has said that in relation to the authorisation of warrants: "The specifics here are that two things will be critical: first, that they decide in the first place that the action is rational and lawful; and, secondly, that it is necessary and proportionate. Those are exactly the same tests as the ones the Secretary of State will be looking at". If it is the case that the Judicial Commissioner will be applying the same test as you, why does the draft Bill specify judicial review test principles?

Theresa May MP: One of the advantages that one has with judicial review principles is that it gives the Judicial Commissioners a degree of flexibility as to how they approach particular cases depending on the impact on the individual of what it is that they are looking at. They will be able to make an assessment and a judgment as to how they wish to approach the evidence that is before them. The Secretary of State looks at the necessity and proportionality of the warrantry. It will be open to the senior High Court judge to look at necessity and proportionality, but under the judicial review provisions they will have the flexibility to determine the way in which they look at that decision. I think that was one of the points that Lord Pannick was making in the article that he wrote before Christmas.

Lord Hart of Chilton: So it would not be right to suggest that the judicial review principles are there in order to prevent a judge from second-guessing the Secretary of State on the merits.

Theresa May MP: No. It will be up to the judge. These will be people who will be well versed in judicial review principles and in exercising those principles. It will be up to them to determine how they approach any particular issue. There may well be circumstances in which they might apply a lighter-touch approach to reviewing a Secretary of State's decision, and others in which they will look more at necessity and proportionality.

Lord Hart of Chilton: It would not come as any shock to you if a particular judge in a particular case, looking at it from his point of view, decides that he would substitute his decision for yours and look from that point of view at the merits of the case.

Theresa May MP: The whole point of the double-lock authorisation is that both parties have to agree to the warrant being approved. If the Judicial Commissioner decides that the warrant should not be applied, having looked at it and applied the tests that they need to apply, then obviously it cannot be operated.

Lord Hart of Chilton: That then would be a true double lock. It would not be a true double lock if the judge was precluded from imposing his decision over yours, because he was looking at the merits and deciding that you had come to the wrong decision, not because of some error or law or—

Theresa May MP: Lord Pannick also noted in his article that judges do accord the Executive a margin of discretion to reflect the expertise in national security matters.

Lord Hart of Chilton: Of course, particularly in national security.

Theresa May MP: They are not re-taking the decision. They are looking to see whether the original decision was flawed. There will be circumstances in which they will determine how they apply that test under the judicial review principles, but it does give them the flexibility to determine that perhaps in one case they might look at it with a lighter touch than they would in another. It is a genuine double lock in that both parties have to agree in order for the warrant to be applied.

The Chairman: Last week, 12,000 miles away at ten past five in the morning, the New Zealand Commissioner—a former High Court judge—who would be the double locker, if you like, in the New Zealand system, said that when he came to applying his mind to a warrant he was not necessarily thinking, "I am a judge and I am going to look at it as a judge", but he was going to look at the necessity and proportionality as well. What you are saying, Home Secretary, is that, essentially, a judge could, and might, look at it in that way too.

Theresa May MP: It will be for the Judicial Commissioner to determine whether the facts of a particular warrant merit the more rigorous review, which could include some consideration of necessity and proportionality.

Dr Andrew Murrison: Thank you for that, Home Secretary, because I think that has reassured a lot of us. Therefore, would it be unreasonable to look at Clauses 19(2) and 90(2), which speak of judicial review rules, since, if we are approaching this on the basis of almost co-equality between the Secretary of State and a Judicial Commissioner and allowing the Judicial Commissioner to have a merits-based approach to this, it would appear that that stringency becomes redundant?

Theresa May MP: The purpose of having the judicial review principles is that it provides the flexibility for the Judicial Commissioner to determine the degree of assessment that they choose to put on a particular application. This was one of the points that was highlighted by Lord Pannick. We are not precluding the possibility of a Judicial Commissioner deciding that they want to give a more rigorous review of a Secretary of State's decision, but they could also determine that in a case they wanted to apply a lighter touch. I am trying not to tie them down, if I can put it like that. They get a degree of flexibility with reference to the judicial review principles.

Baroness Browning: Home Secretary, I would like to ask you about urgent warrants, but, before I do, could I pick up on a couple of points following on from Lord Hart's question? Notwithstanding that the judges appointed as Judicial Commissioners will be very familiar with judicial review principles, would you none the less expect them to receive any kind of training on their appointment? Would they also be subject to any form of appropriate vetting procedure?

Theresa May MP: The individuals who will become Judicial Commissioners will be picked from a group of people who will already have been through certain degrees of checks by virtue of the fact that they have been in the judiciary and are senior members of the judiciary. What was the first question you asked me?

Baroness Browning: Whether they would need any training.

Theresa May MP: I would not expect simply to introduce Judicial Commissioners and sit them in front of these things without some degree of training, which would be explanations about the processes that are gone through in terms of warrantry and things like that.

Q274 Baroness Browning: Thank you. Can we move on to urgent warrants? Why does the draft Bill allow five days for a warrant granted under urgent circumstances to be reviewed by a Judicial Commissioner? Assuming that they are appropriately resourced, why is the period for retrospective review not significantly shorter? Five days seems a very long time.

Theresa May MP: I recognise that there has been some comment on the issue of five days. When RUSI produced its report, I think its suggested that the period that is set should be 14 days. Five days is the current period for any emergency warrant. It automatically has to be reviewed after five days, so five days has been put into the Bill. I am very happy to look at that period of time if that is an issue that the Committee wishes to bring forward.

Q275 Victoria Atkins: Home Secretary, I am dealing now with interception warrants and, first, the issue of modifying interception warrants. Currently, under the Act, when such warrants are modified, those modifications are not subject to judicial authorisation. What safeguards exist to prevent this from being used to sidestep the double lock?

Theresa May MP: There is a limit to what can be considered to be a modification of a warrant. There might be more minor modifications or slightly more significant modifications. The sort of modifications might be the addition of a device to a warrant, for example. The necessity and proportionality of a warrant against a particular individual will have been determined by the double-lock authorisation process. Anything that was in that order would not count as a modification. Anything that required a warrant against a particular individual would require the double-lock authorisation process.

Q276 Victoria Atkins: For my second question I am going to ask you to use your draft Bill because this is a complicated set of sentences that I have to put to you. The first concerns Clause 13(2)(a), which reads: "A targeted interception warrant may relate to a group of persons who share a common purpose or who carry on, or may carry on, a particular activity". Would you keep a finger in that page, as it were, and move to Clause 83(1)(f)? That clause reads: "A targeted equipment interference warrant may relate to equipment that is being, or may be being used, for the purposes of a particular activity or activities of a particular description". It is a very legalistic way of saying, "Could this be used, in effect, to create thematic warrants that could apply to a very large number of people and therefore cannot be classed as targeted?"

Theresa May MP: The answer is no. It will not be possible to use a thematic warrant against a very large group of people.[11] The purpose of a thematic warrant is, for example, circumstances in which perhaps somebody has been kidnapped or there is a threat to life, where only certain information is available, and it is necessary because of the pace at which something is developing to identify the group of people who are involved with that particular criminal activity as being within the thematic warrant.

[11] Thematic warrants may relate to a group of people, but this must always be targeted and must be deemed necessary and proportionate. The size of the group a thematic warrant may relate to will depend upon operational requirements and the necessity and proportionality of what is sought to be gained from the interference. (Witness clarification post-evidence session).

Victoria Atkins: What would the difference be between such a warrant and a bulk interception or equipment interference warrant?

Theresa May MP: Are you now talking specifically about Clause 83 as opposed to Clause 13(2)(a)?

Victoria Atkins: Yes; this is a lawyer's paradise.

Theresa May MP: I am looking a little surprised because, as I see it, there is nothing in Clause 83 that suggests that what is being looked at is a bulk equipment interference warrant.

Victoria Atkins: That is the point. Thank you very much.

Lord Butler of Brockwell: This is on authorisation again. There has been some attention among our witnesses as to the differences between the procedure for authorisation of warrants and modification of warrants between the intelligence agencies and law and order. This relates to equipment interference and it carries on from the question about interception. In the case of equipment interference warrants, the intelligence agencies require a warrant from the Secretary of State plus the Judicial Commissioner, and with law enforcement similarly it has to be a chief officer and the Judicial Commissioner. In the case of modifications, it is different. For intelligence, it is not subject to approval by the Judicial Commissioner, whereas for law and order it is. What is the reason for treating modifications of warrants differently between the agencies and law and order?

Theresa May MP: With regard to modifications to the different warrants from either the agencies or from law enforcement, modifications to the agency warrants require approval from the warrant issuer, which is the Secretary of State or designated official, so that they are being looked at independently from the agency. Where there is modification to law enforcement—and I may have missed the point of the question—the issuing authority is the internal law enforcement chief. To give the independence, that is why we have instructed that the Judicial Commissioners should also authorise modifications for law enforcement equipment interference warrants. It is about getting that degree of independence but it can be achieved in different ways.

Lord Butler of Brockwell: I see, but I wonder why there are different ways.

Theresa May MP: In relation to the agencies, the process is the one that exists at the moment, on which there have been no concerns expressed as to how it operates. As I indicated in response to Ms Atkins, when we are talking about modifications, we are not talking about something that opens up a whole new warrantry in relation to, say, an individual, but it might be something like another device being placed on the warrant.

Q277 Lord Butler of Brockwell: Thank you. In the case of the technical capability and national security notices, these are not subject to the double lock. Why not?

Theresa May MP: The double-lock authorisation is there where there are processes that are intrusive into an individual. When you look at the technical capability and national

security notices, those are of a different order. They are not about that question of the intrusion that is taking place into an individual.

Q278 Stuart C McDonald: I have one or two questions about extraterritoriality, please, Home Secretary. A number of witnesses, both in their written and oral evidence, have expressed concern that there is not very much in the Bill about these issues. First, dealing with the question of the UK sharing information abroad, what safeguards are there to limit what can be done in that regard?

Theresa May MP: We look at the handling arrangements that are in place when we are sharing material with overseas partners. It is Clause 41 of the draft Bill that sets out that, before intercept material is shared with an overseas authority, the issuing authority sharing the material must be satisfied that they have appropriate handling arrangements in place to protect the material, equivalent to those that apply under Clause 40. Those might not be exactly mirrored; they might not be absolutely the same; but they are equivalent, so they give the same degree of appropriate handling arrangements.

Stuart C McDonald: But it is a matter for the appropriate issuing authority to decide. Is that not quite weak? Can we not strengthen that in the Bill?

Theresa May MP: We are confident that the appropriate issuing authority has this requirement on them and therefore will ensure that these are in place. I recognise that the joint scrutiny committee will be reporting.

Stuart C McDonald: Thinking of things the other way round—the United Kingdom obtaining material obtained through interception overseas—am I right that that is essentially going to be down to codes of practice? Again, there is a lot of criticism that that is not satisfactory.

Theresa May MP: Do you mean in terms of the United Kingdom issuing warrants in relation to an overseas provider?

Stuart C McDonald: Yes. The evidence of Amnesty International, for example, is that there are no provisions at all in the Bill dealing with the receipt by the United Kingdom of material obtained through interception by overseas partners other than in Schedule 6. Schedule 6 provides a bare statement that codes of practice will "cover the process" for overseas requests and handling data received from them. Is it down to the codes of practice, essentially, to govern that?

Theresa May MP: There will be codes of practice. The reason I asked the question was to try to clarify exactly what sort of circumstances we are talking about in terms of extraterritoriality.

Stuart C McDonald: Interception.

Theresa May MP: In relation to an interception, we repeat the position that we put into DRIPA that has always been asserted by all Governments in relation to the ability to exercise a warrant against a company that is offering services in the United Kingdom and binding them by the law of the United Kingdom. That will be a lawful warrant that would

be applied to a provider. Information obtained under that warrant would be similar to information obtained under a warrant that was issued domestically.

Stuart C McDonald: I think these witnesses are getting at information that was obtained by security and intelligence services of other countries. Correct me if I am wrong, but, unless the Bill says something about this, there could be protections that prevent our security and intelligence services obtaining information on certain people because of all the protections that you have set out in the Bill. It would drive a coach and horses through the Bill if they were then able to simply go and obtain this information from the security intelligence services of neighbouring countries. Is there anything in the Bill that governs how these relationships work?

Theresa May MP: We have been very clear in ensuring that where information is obtained it is done so against an appropriate legal framework. There are provisions in place that ensure that the agencies operate and only obtain information where it is lawful for them to do so.

Stuart C McDonald: Where do we find that legal framework? Am I right in thinking it is all down to international treaties, some of which we know about and some of which are perhaps not in the public domain?

Theresa May MP: There are various aspects to the legal framework against which the agencies operate. If I can be of more help in writing to the Committee—

The Chairman: Thank you, Home Secretary. I am going to have to move on now—because I know you are pressed on time—to privilege with Lord Hart.

Q279 **Lord Hart of Chilton:** It will not surprise you at all to know that there have been many who have complained of the limited protection for legal privilege and for journalistic sources. I want you to explain to us why it is that you cannot put legal privilege, which plays an important part in the rule of law, in the Bill itself rather than relying upon a code of practice, which as yet is unpublished. Dealing first with legal privilege, why is that necessary?

Theresa May MP: It is important that the law enforcement and the agencies are able to use these powers in circumstances where it is necessary and proportionate for them to do so and not to exclude the use of these powers in any particular sets of circumstances. You mentioned both legal professional privilege and the question of journalistic sources. Of course, we are making specific provision for certain circumstances in relation to journalistic sources, but the significance of the relationship between an individual and lawyers in discussing matters is always recognised. I do not think it would be right to say that these powers could never be applied in those circumstances. It is right that, again, it is a question of judgments about necessity and proportionality.

Lord Hart of Chilton: There is not much evidence base in all of this. How many times has the Home Office had to interfere with legal privilege? How many times has that happened? Is it a very tiny fraction of numbers?

Theresa May MP: You used the phrase “interfere with legal privilege”. We are not actively interfering with legal privilege, but I am sure everybody would agree that you could not

accept a situation where you said, in regard to anybody who had any legal qualifications and who might be operating in a relationship relating to those legal qualifications with an individual, that these powers could never be used in those circumstances, because, I am sad to say, you may very well find that there are circumstances in which people who are legally qualified and operating in those are potentially providing support to some people who would perhaps be involved in, for example, criminal activities.

Lord Hart of Chilton: Of course, if they misuse privilege, they are not able to call upon it to be used as a defence. It is not a universal rule. If you are a naughty lawyer, you cannot claim legal privilege.

Theresa May MP: Yes, and sometimes it may be necessary to use some of these powers to identify that you are a naughty lawyer in the first place.

Lord Hart of Chilton: I go back to the question: is there an evidence base where you have done this?

Theresa May MP: There is, I think, an important point of principle in the ability for law enforcement and agencies to have these powers and to be able to exercise them in particular circumstances. If we go back to remembering exactly why it is that they have the ability to exercise these powers, dealing with crime and with terrorists who would seek to do us harm, it is important that these powers are available. We do not publicise figures in relation to particular types of warrants or the interception that is undertaken by those warrants. Indeed, under RIPA, it is an offence to indicate whether a warrant is in place in a particular circumstance or against a particular individual.

Lord Hart of Chilton: The point being made by many people is that for you to interfere with legal privilege it should be on the face of the Bill and not in a code of practice.

Theresa May MP: I think that the arrangements that we are putting in place are appropriate for the reasons that I have set out.

Q280 **Lord Hart of Chilton:** I will not press you any more on that. The last of the trio of questions in relation to that is that the Wilson doctrine is not enshrined in the Bill and it does not require the Prime Minister to make a declaration to Parliament. Why was that safeguard left out of the Bill?

Theresa May MP: The Wilson doctrine has been recently tested before the Investigatory Powers Tribunal. It was found that the Wilson doctrine was still in place and that the definition of the Wilson doctrine was as I had set out to the House of Commons. The important element of the Wilson doctrine that will be in the Bill is that it will be a requirement, where it is suggested that there be interception in relation to not just a Member of Parliament but Members of the House of Lords, UK MEPs and Members of the devolved assemblies and parliaments, that where that is going to be the case the Prime Minister must be consulted on its use.

The issue as to the aspect of the Wilson doctrine that was about the Prime Minister making a statement to the House when policy changed in relation to the Wilson doctrine is of a

slightly different order. The Prime Minister has been clear that that still applies. I do not think it is appropriate to put that on the face of a piece of primary legislation.

Lord Hart of Chilton: I suppose it is part of a subset of accountability to Parliament. If you do not make a statement to Parliament, you have simply considered the question. It is not quite the same.

Theresa May MP: I am not sure whether there is some misunderstanding about the nature of the Wilson doctrine in the statement to Parliament that the Prime Minister makes. The statement to Parliament that the Prime Minister makes is not that there has been the interception of a number of Members of Parliament. The statement that is in the Wilson doctrine is about whether the policy that has been adopted is different. As to how these matters operate, statements about changes of policy on a whole range of matters are regularly made to Parliament. But that is not a requirement that is on the face of any legislation in any area in which we operate.

The Chairman: There are some other questions, but I know your timing is difficult. Are you able to answer any more?

Theresa May MP: Yes, for a short period. I have a speaking engagement on the Estate, to which I will have to go shortly, but I can take a few more.

The Chairman: Ms Mahmood, can you be quite precise, as you always are?

Q281 Shabana Mahmood: I will be, Lord Chairman. On Judicial Commissioners, the system for appointing them by the Prime Minister for a term of three years is different from the way in which other senior judges are appointed. Why is there a difference between the two?

Theresa May MP: The commissioners currently are appointed by the Prime Minister. You are talking about the Judicial Appointments Commission specifically.

Shabana Mahmood: Yes.

Theresa May MP: Yes, there will be some circumstances in which one might be looking at a sitting judge being appointed, in which case it will be a matter more for the Lord Chief Justice and for advice from the Lord Chief Justice. Indeed, the intention is that the Lord Chief Justice would be making nominations to the Prime Minister.

Shabana Mahmood: Are you not worried, given the controversial history of the Bill, with what happened in the last Parliament, that there is maybe the appearance that the Judicial Commissioners might have a reduced sense of independence from the Executive? Is that a concern to you? Is that something you would like to avoid?

Theresa May MP: I recognise the importance of people seeing the independence of the commissioners. The current commissioners are appointed by the Prime Minister. There is no suggestion that they have not been independent in the operation of the work that they have done. I do not believe that the appointment by the Prime Minister would jeopardise in any sense the independence of the Judicial Commissioners in the future. They will, as I say, be people who have been or are senior members of the judiciary, and there will be

circumstances in which the pathway with the nomination by the Lord Chief Justice is more appropriate than the Judicial Appointments Commission.

Q282 Shabana Mahmood: Thank you; that is helpful. One of the arguments that has been made to us is that the function of authorisation and oversight being done by the same people might give the appearance that the commissioners are effectively marking their own homework. Is this something that has been put to you? Is it something you are concerned about?

Theresa May MP: We have thought about this issue. We already have an example, through the Office of Surveillance Commissioners, where they are performing two functions. There will be two functions and, therefore, two sets of people within the Investigatory Powers Commissioner and that office—those who are undertaking the authorisation process and those who are undertaking the inspection process. There are some benefits for the ability of those to interact, to understand some of the issues of practice, but it is important that they keep their functions separate. Because we have an example of how that is done already with one of the offices, it is perfectly possible for that to be done in a way that maintains their independence. I am tempted to say, given that we are talking about Judicial Commissioners, that I am sure they will fiercely defend their independence and the necessity of keeping those functions clear.

The Chairman: Thank you very much. We will probably have to stop there as it has been nearly two hours. It has been very informative. It has been exhaustive but I hope not exhausting. Thank you very much for coming along. We now look forward to compiling our report, which you will see in due time. Thank you very much again, Home Secretary, for coming along.

Theresa May MP: Thank you, Chairman.

Tim Musson, Law Society of Scotland (QQ 137-144)

Evidence heard in public Questions 137-144

Oral Evidence

Taken before the Joint Committee

on Monday 14 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Stuart C McDonald MP, Matt Warman MP, Baroness Browning , Lord Butler of Brockwell, Bishop of Chester, Lord Henley, and Lord Strasburger.

Witness: **Tim Musson**, Law Society of Scotland, gave evidence.

Q137 **The Chairman**: A very warm welcome to our witnesses today. I know there was not very long notice for everyone, but thanks to all four of you for coming along to give your thoughts on what is regarded as probably one of the most significant Bills of this Session. As in previous sessions and in any similar parliamentary committee, we will ask you a number of questions, which I hope will stimulate your brain cells. We will have a dialogue with you in this particular session about the importance of privilege to the legal and journalistic professions.

I am going to start by asking a question about the legal professional privilege. How do you think the draft Bill addresses the concerns of the legal profession about privilege and the investigatory powers in England, Wales and, of course, Scotland? Does it create any new issues?

Colin Passmore: It falls to me, as the lawyer among the four of us, to see if I can address that. My name is Colin Passmore. I have been a solicitor for 31 years now and I can modestly claim to be an expert on privilege because I write the leading textbook. I am sad enough to know the thousands and thousands of cases on privilege and the hundreds and hundreds of statutes that deal with privilege. What is unique about RIPA and this Bill is that, on the face of it, they do absolutely nothing to address the concerns that the legal profession has about privilege and the way in which surveillance techniques in all their glory can be used to infringe the privilege.

Privilege, as I am sure you know, is possibly the highest right known to the law. It is over 500 years old. It is jealously guarded, not only by the legal profession but by the courts, with the result that there are usually hundreds of cases in London alone every year in which challenges to privilege are upheld. In addition, in every single statute that confers investigatory powers of any sort, whether we are talking about the police, the SFO, the Revenue, even local weights and measures departments, there is always a provision that actively protects privilege, so nobody—the police, the Revenue—has the ability to force any client to divulge their privilege. The same thing happens in statutory instruments. This draft legislation and its predecessor are unique in that there is nothing in them that protects privilege.

When this issue came before the House of Lords in the McE case from Ireland some years ago, it is fair to say that the legal profession was extremely surprised that Section 27 had the ability to enable the security services, the police and others at least to listen in to privileged communications in certain circumstances. Even the House of Lords in that case indicated a great reluctance to interpret Section 27 as giving the ability to listen in on privilege, but the House of Lords proceeded quite clearly on the basis that this happens very, very rarely. The House of Lords was at pains to say that if it happens on a regular basis there will be a chilling effect on privilege. The chilling effect is really important, because it inhibits the frankness of clients, whose right it is, with which they speak to lawyers. If that chilling effect is in play, it could undermine the right to a fair trial under Article 6, infringing on privacy rights under Article 8, and undermining the administration of justice.

We know now, from cases like the Belhaj case and other cases that have come to light in the last year, that whereas we thought this interference with privilege was very, very rare, it is happening far too often and on a routine basis. In my view and the Law Society's view, unless this legislation is amended so as to deal with privilege on its face, then privilege, this very old and supremely unique right—there is nothing else like it in any form of communication—begins to become seriously undermined.

The Chairman: Mr Musson, do you want to add anything to that?

Tim Musson: Not a great deal, Lord Chairman. My background is not legal professional privilege in the same way as Mr Passmore's. I am here to represent the Law Society of Scotland. It appears that legal professional privilege in Scotland is very similar to that in England and Wales. The differences are absolutely minimal, although it has arisen in a slightly different way. There are the two sides to the privilege: England started on one side, Scotland started on the other side, and they have come together. Certainly the Law Society of Scotland is very concerned about the erosion of legal professional privilege that appears to be quite possible with this Bill. They have great concerns about it, which do not differ in any way from what Mr Passmore was saying.

The Chairman: Picking up on where Mr Passmore finished, and now that you have added to his comments, it is very appropriate for our only Scottish member to come in on the issue of any possible amendments.

Q138 Stuart C McDonald: Mr Passmore, you suggested that this Bill will need some amendments before you are happy with its approach to privilege. Can you give us any more indication of what sort of amendments you think would be required?

Colin Passmore: There is a serious question as to whether there should be a prohibition on interference with privilege at all. Why is this interference necessary? I respectfully suggest that there are not many cases where lawyers, be they solicitors, barristers, advocates, have been found guilty of abusing the privilege. If a solicitor or a client in their relationship with a solicitor abuses the privilege, the privilege falls away. There is something known as the crime-fraud exception or the iniquity exception.

You do not need these seemingly open powers to listen in to solicitor-client conversations unless you have some evidence that there is something wrong going on. There is very little evidence that solicitors or lawyers abuse the privilege, and therefore the power to listen

in, to intercept or to hack is simply, in my view, unnecessary. I would be a strong advocate, and the Law Society is a strong advocate, joined by Scotland and indeed other jurisdictions, for having the type of privilege preservation clause that you find in all other statutes, including those that deal with police powers, revenue powers and so forth. I respectfully suggest that there needs to be a provision in here that makes it clear privilege is out of court.

Stuart C McDonald: Are you frustrated, then, that sometimes we hear from the Home Office that they are scared of putting some kind of prohibition on intercepting legal privilege because of the risk of abuse? You are saying to us in effect that that abuse means that the privilege no longer applies.

Colin Passmore: That is my view. I know many lawyers who understand the importance of privilege and its unique status as a means of privacy in communications with clients. Many lawyers whom I know take the obligations that arise from having the benefits of privilege very seriously. I can think of a handful of cases in which privilege has been abused; I am aware of one, which came to my attention this morning, that has just gone up to the European Court of Human Rights. It simply, in my view, does not happen that lawyers abuse the privilege.

Stuart C McDonald: Mr Musson, do you also seek that prohibition in the Bill?

Tim Musson: Ideally, yes, I would seek that. If it cannot be taken as far as that, there become issues about who is competent to permit interception of these communications. It would need to be someone who understands legal professional privilege, and the sort of person involved in this authorisation might not have that knowledge or understanding.

Q139 Lord Butler of Brockwell: Mr Passmore is making the case for prohibition on the grounds that privilege falls away if a lawyer is engaged in criminal activity. In those cases, you would say that there must be evidence that that is happening, but then you are putting too much power in the hands of the authorities, are you not? They say, "We have evidence"—let us say this is the Home Secretary—"and, therefore, please may we have a warrant to listen to this lawyer because we think privilege has fallen away?". Would you not rather have a stronger safeguard than that, a formal procedure that certifies that that is the case, rather than just the judgment of the Executive?

Colin Passmore: That is a good point. I do not make the case just on the basis of the iniquities exception. I make the case primarily on the sheer importance to the administration of justice of the privilege itself. I am very concerned that this Bill has the ability to undermine privilege more generally. With regard to your second point, in the way this iniquity exception works with, for example, the police, the SFO or the Revenue authorities, when they seek a warrant to go into a solicitor's office, they have to satisfy the judge in the Crown Court that there is a really good case for being able to go into the solicitor's office, knock on the door and start to take papers away.

Forgive me, I am going slightly off your point but I will come back to it. If privileged materials are identified, whether or not the exception applies there is always an independent lawyer in attendance who will do the physical bagging up of the documents or the computer disks, and he or she will later go away to determine whether they are privileged. There should be

a check, of course, but a judge is more than capable of looking at the evidence as to whether or not the iniquity exception is likely to apply. Judges are very good at this.

Lord Butler of Brockwell: Would that not be covered by the new procedure under this Act: that if the Home Secretary is to grant a warrant, it has to be endorsed by a judge?

Colin Passmore: Yes, as long as the reference to the judicial review standard is removed—first, because that introduces an element of ambiguity: what is the judicial review standard? I know that eminent lawyers such as David Pannick have written to say that it is fine; I know many others who disagree with that. But I am not even sure why we need that. If the communication that the authorities wish to intercept is subject to the iniquity exception, that of itself should be enough; we do not need a judicial review standard. Does the exception apply prima facie or does it not? If a judge is not happy that the exception applies, the warrant or the ability to intercept simply should not be granted.

Lord Butler of Brockwell: That, if I may say so, raises a slightly different point. I am not trying to put words in your mouth, but I think you are saying that if the judicial review test was removed, you would be content with a procedure whereby the Home Secretary can grant a warrant, provided it is endorsed by a judge, if there is a really good case?

Colin Passmore: Coupled with an express recognition in the draft Bill, in the statute, that privileged material is not available, that would be great. I would be happy with that and I think the Law Society would be.

Bishop of Chester: The closest parallel might be a confessional and a priest. It is humorous on one level but serious on another. It is on a much lower level than legal privilege, but what qualification there is to an iniquity exception is a matter of contemporary discussion. It may apply only to the Church of England, but we have other religious groups in our country now. I would have thought that if we are going to put something in the Bill, in principle we should, I suggest, at least look at whether that is a parallel set of circumstances, because putting a bugging device in a confessional situation raises the same sort of issues in a different context.

Colin Passmore: It does. I am sorry to disappoint you, but the law addresses privilege as a higher right capable of greater protection than the confessional box. It is easier to get disclosure of your conversations with a confessor than it is my conversations with my client. I am not saying it is very easy; it is very difficult, but I am afraid privilege is on a slightly higher plane so far as the English and Scottish courts are concerned.

Victoria Atkins: To clarify, on the point of the iniquity exception, your evidence is that you wish protection to be put into the Bill that reflects the law as it stands currently across all other statutes, so if a solicitor is trying to commit a crime with their client, that information will not be protected by privilege?

Colin Passmore: Absolutely right. It cannot be protected.

Victoria Atkins: You gave the example of search warrants. Interception warrants are a much rarer event even than the pretty rare event of HMRC or whoever going into a lawyer's office. The safeguards are there, surely, for interception warrants, given how rarely, particularly in secure environments and so on, these are used.

Colin Passmore: The occasions that we know of when cases in which the police have sought interception warrants have come before the courts are relatively rare, and you have to go through the Crown Court judge warrant procedure and satisfy the judge that the iniquity exception is likely to apply. I am a long way from being an expert on interception and the security services, but I have been slightly horrified this year at the number of cases, starting with Belhaj and others, that have come before the IPT in which these issues are raised. I am not myself convinced, although I am not an expert—far from it—that these cases are such a rarity. I would therefore far rather the security services et al had in the Bill the clear recognition of just how important privilege is, plus the mechanism of going via the judge.

Q140 Suella Fernandes: Thank you for your evidence today. Do you agree that someone who belongs to one of these professions that we are talking about, maybe the legal profession or the journalistic profession, may also, albeit in rare cases, pose a threat to national security, and in those cases it is important that the agencies have a power to intercept their communications?

Colin Passmore: I find it difficult to think of a case that would be any more than a rarity. I am aware of one case in Northern Ireland, which is the case I alluded to earlier that has just gone up to the European Court of Human Rights, where a solicitor conspired with his alleged terrorist client to bump off a witness. That is incredibly rare. It is so rare it is shocking. I am not aware of any cases where that is likely to happen. I am not suggesting for a moment that every single member of the legal profession in the UK is beyond reproach—of course not—but I find that a difficult concept to get my head around.

Suella Fernandes: Do you appreciate that the agencies have given evidence that they would never specifically seek to acquire privileged material except when they apply for a specific warrant?

Colin Passmore: I would give you the lawyer's answer to that, inevitably, which is that if that is the case, they cannot have a problem with the Bill recognising the importance of privilege. In other words, if they recognise that they do not want privilege, let us put it in here and make sure it is beyond doubt. Then, if there is a circumstance in which the iniquity exception applies, go to your judge for your warrant. If your evidence is good enough, fine, you are up and running.

Suella Fernandes: Lastly, it is always subject to the test of being necessary and proportionate and that the intelligence cannot be obtained in a less intrusive way.

Colin Passmore: That I disagree with. The courts and some very famous names in the judiciary, such as Lord Denning—I am showing my age—and others since have recognised that the consequence of a claim to privilege is that the court, the Revenue and the police are deprived of what they regard as potentially relevant evidence. It is a consequence that we have to face with an assertion of privilege.

Bob Satchwell: I think your question was: could it be possible? It would be foolhardy of me to say that it was impossible, but it would be astonishing. There are so many examples of the way journalists understand and very carefully apply restrictions upon themselves in relation to national security issues through the DSMA committee, through what were

wrongly called D-notices, and things like that. We work like that all the time. I have never known of a journalist who would ever have put someone's life or national security at risk inadvertently. What we are concerned about is precisely the point that there need to be very clear procedures and rules if someone is seeking to invade the journalist's activities and his sources. More recently, and perhaps we will come on to this, the evidence has been that some organisations rode roughshod over something that we all thought was accepted.

Q141 Victoria Atkins: What is the legal status of the codes of practice under RIPA?

Colin Passmore: Vague. They are the worst option for dealing with this issue, in our view. We have a problem here at the moment in that the codes of practice that will be developed pursuant to this are so far unwritten, although I imagine they are going to reflect a lot of what is in the present codes. A code of practice is what it says on the tin: it is a code. We have seen from recent cases where the security services have breached the code that there is not really a sanction. There may be some disciplinary sanctions, but we have seen that the remedies available in the ITP are pretty low-key compared with what one might expect to get, for example, in the High Court, where there might be a claim arising out of a breach.

They are clearly not of the status of legislation. In the absence of something in the Bill, something in the Act to be, that makes the status of privilege clear, the code of practice is always going to suffer, in our view, from this weakness that cannot be cured, no matter what you put in it. It is a code. It is slightly better than the *Highway Code*.

Victoria Atkins: Should we not separate between security services and law enforcement on this issue? As you know, under the codes of practice for the Police and Criminal Evidence Act, there are very real ramifications for the prosecution if the police fail to follow the code. The case may be dropped.

Colin Passmore: I totally agree, but the big difference is that the Police and Criminal Evidence Act, or the Criminal Justice Act for the SFO, makes it clear that privilege is untouchable. You have this primary legislative direction that we do not have here, nor with RIPA. Therefore, the codes of practice are bound to suffer from that. The codes of practice currently have all lovely things about privilege, but they are effectively unenforceable. You have to trust the operatives in the security services to make sure that they will obey them and that they will adhere to them. Personally, I do not think that is good enough when we are dealing with privilege, which as I keep saying is this extraordinary right, which should be protected in the primarily legislation.

Victoria Atkins: What do you expect to be contained in the codes of practice issued under this Bill?

Colin Passmore: That depends what is in the Bill. I would like to see in the Bill: a recognition that privilege is untouchable and that therefore there should be a fair amount of guidance to the security services and others on what privilege is, why it is so important and what the consequences are of coming across it: a very clear statement, if I may suggest, that there is no basis whatsoever for targeting it deliberately; a very clear explanation of what the iniquity exception should be; and a very, very clear statement of the dangers of playing fast and loose with privilege. You may ultimately cause a trial to be stayed because you have interfered with a defendant's right to a fair trial; you have interfered with his or her

privilege. There would need to be a lot, in my view, in the code of practice. I do believe that it has to emanate from the primary direction in the Bill as to the importance of privilege.

Victoria Atkins: I have a final question on that. The commissioners will play a very important role under the draft Bill as it stands at the moment. Is it not sufficient to trust them with bearing that very much in mind when they are looking at individual applications, and in due course reviewing how the legislation is being applied generally?

Colin Passmore: The intent of the legislation is that there would be a senior judicial officer, at least at Court of Appeal level or above, so really senior, experienced lawyers. Provided they also have the direction in here that privilege is untouchable unless the iniquity exception is in play, I would be happy with that.

The Chairman: Thank you very much. We turn now to journalistic provision and privilege, touched on Clause 61 of the Bill.

Q142 Suella Fernandes: Clause 61 requires that a judicial commissioner approves the issuing of any warrants for obtention by agencies. What is your view of that safeguard in protecting the media's rights?

Bob Satchwell: Our simple view is that it does not go far enough. Some interim measures have been put in place to do with RIPA and so on, but the difficulty is that RIPA was used—I have always argued that it was misused, actually—in certain cases, some of which became very full of headlines and so on, to get around the good safeguards that are in PACE. A number of examples that learned lawyers have come up with—I am not a lawyer, by the way—show that that happened.

The key point with legislation of this kind is that we know what the basic intention is in these troubled times, but that is why legislation was enacted previously. I remember when RIPA was enacted it was made clear to me by Ministers whom I talked to, and I believe it was the will of Parliament, that RIPA was supposed to be an Act to do with fighting terrorism. We have found that, in fact, it became something completely different.

I start by saying that it is very important that the legislation—with all due respect to those who may have been involved in that legislation originally; no one expected that it would be misused in the way it came to be misused—is very clear what the ground rules are before you even get to the codes of practice. Codes of practice are fine so long as someone follows those codes of practice. It absolutely needs to understand, as most people understand—it is something I have always had in my mind, and I have been 40 years a journalist—the first rule of journalism: that you protect your sources. That is in other parts of legislation. It is understood in Europe. It is understood in most places. Judges will very rarely make a journalist reveal his sources, and so on. That background has been totally misunderstood by the police for example, who have ridden roughshod over those principles. Somehow it has to be there very, very clearly.

Going back to your previous question about the possibility of a journalist being involved in something that was against the national interest, they have to come up with evidence, not a fishing expedition; it has to go before a judicial authority. What is more, there has to be

an opportunity for the media organisation to argue and to explain the case, because it is not just a matter of delving into journalist records or into who those sources are.

An inquiry into certain parts of a journalist's activity may inadvertently reveal a source that the police or the security services are not interested in. That is why it is very important that there is an opportunity to know when the police or the security services are asking for that, and an ability to argue that case.

The Chairman: Mr Smith, do you want to comment?

Andy Smith: Yes, just to pick up and elaborate on a couple of things that Bob has said. The NUJ agrees that, while not ideal, the provision under PACE is one that we have been able to work with. We have been able not only to oppose some applications outright but to use the knowledge that we have as journalists to explain the situation that we are in, so that a judge can make a variation of something in front of him, which, as far as I can see, is very difficult under the framework that you have in front of you. A police force may come and ask for hundreds of hours of video tape and end up with 10 or 15 seconds that the judge considers to be pertinent to the application they have made.

To be clear, what we have under PACE, as Bob said, is: prior notification, which we think is absolutely essential; sufficient information about the application, for instance what other means have been attempted to obtain the information, so that we are treated not as a first resort but as a last resort; the importance of a face-to-face hearing, which is not about journalists having their day in court but about being able to demonstrate, particularly to potential sources of information, that the journalist's commitment to protect their sources goes up to defending them in open court and going to bat on their behalf; and a rigorous right to appeal before approval is granted. Under the draft legislation, there is an ability for the force or body making the application to appeal, but there is no right to appeal for any of the persons affected, simply because they are not told.

The only other point I would make initially is on the business of communications data, as opposed to the information contained in the communication itself. Journalists are in a very particular position, in that very often the information gathered has already been published and the most important thing is the fact of the communication. The communications data is at least as important as the content of the communication, quite possibly even more so, given our commitment to protect journalistic sources. It is a very particular situation that journalists are in in that respect.

Suella Fernandes: I have one final question. Special protection requires special responsibility, and in some professions the communications between the professional and their client are very well-regulated, for example the medical profession or the legal profession. There are regulations covering journalists, but they are very different from the regulations that apply to the other professions. Do you agree with that?

Bob Satchwell: Yes. It is quite reasonable. Journalism is not a profession in the sense that the professions are professions. It is not a closed shop in that sense.

The Committee suspended for a Division in the House.

Bob Satchwell: But I hope that we always act professionally, which is somewhat different. In all the codes of practice that journalists have, whether for newspapers and magazines or in broadcasting and so on, there is a simple recognition that the protection of sources is a moral duty, as it is put. That is recognised by the courts, by European authorities and so on.

Andy Smith: The other thing PACE does is concentrate on journalistic material. If a journalist, however they want to label themselves, is doing anything that is outside of that journalistic function, it is not covered. Bob talked about the times when legal privilege falls away, and, in a similar way, material that the police want to access concerning a journalist doing something other than their job would not be covered.

Suella Fernandes: The point I want to make is that there is much less regulation for journalists compared to the other professions, and the definition of a journalist is not as clear cut as it is for members of the legal or medical professions.

Bob Satchwell: That is true, but just because the regulation is not quite as formal does not mean that it is not followed. In some circumstances, the following of journalistic practice, which is accepted across the industry, is stronger because it is not laid down in legislation. The fact that it is peer judgments means that people will adhere to it.

On the question of sources and the release of information, it has been recognised in legislation and it is recognised in the courts that sources and other journalistic material should be delved into only in special circumstances.

Q143 **Matt Warman**: I should declare an interest. I am a member of the NUJ, although, I suppose, a recovering journalist. To start off with, what is a journalist these days? Would you include bloggers? Would you include someone live-tweeting this Committee who is effectively a member of the public? Where might we draw that line?

Andy Smith: To go back to what you were saying, there is an interesting debate to be had on that. I have seen various definitions. The advantage of PACE is that it does not define a journalist, and in some ways that is safer. If that definition is to develop as the technology develops, I would rather see that debate happen as a matter of developing case law, which would involve open hearings rather than conversations behind closed doors that make decisions arbitrarily, or not arbitrarily, about whether somebody who, for instance, had a regular blog and followed our own code of practice but was not paid for it would be described as a journalist. Frankly, some very good journalistic work is being done on the internet by people who are not associated with the traditional media outlets. There is a debate to be had there, but I would say it is developing.

Bob Satchwell: There are probably some common-sense definitions. It is difficult to define now, but, as Andy said, it will be developed in law. That is one of the reasons why there needs to be an ability to argue a case and say whether this person is a journalist or not. That is part of the principle that is there. I can see that some authorities would say, "We did not know he was a journalist. We just did it". That is the difficulty: that people will try to go outside what has been accepted practice in the past. It would be difficult to define absolutely what a journalist is.

Matt Warman: Bearing in mind that as-yet-undefined elasticity, how could we amend the Bill in front of us to achieve some of the things that you are talking about?

Bob Satchwell: There will be a submission from the Media Lawyers Association, which will come back in huge detail on this. Please excuse me for not having all that legal background. They will come up with some very clear suggestions on that.

Matt Warman: Mr Smith, did you want to add anything to that?

Andy Smith: Like Bob, I am not a lawyer. I would not want to start amending it for you, but the principles would involve something like "somebody who is regularly practising" or "employed". Those sorts of phrases would allow you to separate out those who are simply expressing an opinion on a blog on a regular basis from those who are engaged in journalism.

Q144 Mr David Hanson: Could you comment on what happens when a journalist is undercover and is acting as a journalist but is not, to the public knowledge, acting as a journalist at that particular time? The fake sheikh has been mentioned, but there may be other examples that we are aware of. I am interested, again, in the definition in relation to the Bill.

Bob Satchwell: In most cases, they will be employed or commissioned to be doing something undercover, and there will be some governance surrounding that from the person who has hired or commissioned them to do it. There are some difficulties if people are just going off on their own and doing it—difficulties for themselves, indeed—and they do not have the protection of an organisation behind them. That is what normally happens.

Andy Smith: The NUJ code of conduct is very clear in stating that investigations should be done by open means wherever possible and that any subterfuge has to be justified in terms of an overarching public interest, so you cannot simply decide to go away and pretend not to be a journalist because you feel that it will be the easiest way to get hold of the information.

Bob Satchwell: It is covered by virtually all codes across the media that you have to have a very good reason for subterfuge. In the new editors' code at IPSO, it is very clear that there is governance on that: at every stage of involvement in an investigation of that kind, notes have to be taken at the time about what the public interest was. It will be recorded and they will be audited on that.

The Chairman: Thank you, all four of you, very much indeed. It was very informative and very useful, and the Committee will be looking carefully at the written evidence that you will be providing us as well.

Shami Chakrabarti, Director, Liberty (QQ 127-136)

Evidence heard in public Questions 127-136

Oral Evidence

Taken before the Joint Committee

on Wednesday 9 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Lord Henley, Lord Strasburger.

Witness: **Shami Chakrabarti**, Director, Liberty, gave evidence.

Q127 The Chairman: A very good afternoon to you—or evening, now. I am sorry that we are a little late—there was a vote in the Commons earlier. You are very welcome. I will make two points before I ask the first couple of questions. My colleagues will come in after that. Each of you has given your response to the Bill very publicly over the last number of weeks. The Committee has all the statements that you have made. In addition, of course, I am sure that you will give us written evidence. This is a very big Bill. It is very lengthy and very technical. Has subsequent analysis of the draft Bill led any of you to alter any of your positions from those that were taken in your initial response to the Bill's publication?

Shami Chakrabarti: I would simply say that I am possibly more alarmed by the Bill than I was at first glance. The Committee will appreciate that it is a long Bill.

The Chairman: Very long.

Shami Chakrabarti: It is very complex. Like all legislation, it requires an understanding of what its clauses actually provide, as opposed to how its clauses have been pre-briefed or spun in the press. It also requires a level of understanding of the relevant technology. Those two things have to come together. My own organisation is a human rights organisation with, traditionally, considerable expertise in legislation, but recent weeks have given us the opportunity to work with partner organisations that have a considerable level of expertise in the technical sphere. That experience makes me more alarmed now about the personal and cybersecurity implications of the provisions, however laudable and well-meaning they may be in their motivation.

The Chairman: Do your colleagues share that view? Are you more alarmed now, as the weeks go by?

Renate Samson: Initially I was very clear that there was a lot to read. I have now read through it. The implication was that there was a lot of transparency. At first, it seemed that that was the case, but, as you read more and more, you find that there are a lot of vague terms in the Bill that require a lot of head-scratching to try to understand exactly what may be meant. Trying to engage the public in understanding what the Bill says and what its

implications for them will be has been a challenge. There probably need to be many more readings of the Bill before you can get to the bottom of even a tip of what might have been meant.

Caroline Wilson Palow: I agree. We did and do welcome the opportunity to engage in this process. As we have started to get into the Bill, which is long and complex, we have started to notice a few things. For instance, Part 6 is about bulk powers, but when you look into some of the other particularly targeted provisions, you start to see that aspects of those look quite a lot like bulk powers in and of themselves. The service provider provisions that are sprinkled throughout the Bill put a lot of obligations on service providers, which I know you have often heard about, and which seem like they could undermine both security and trust. Those were not things that were necessarily apparent when we first took a look at the Bill. Another particular provision that concerns us a bit is Clause 188, on national security notices, and how that will play out in conjunction with the other provisions of the Bill.

Jim Killock: We have been particularly alarmed by the reintroduction of the so-called filter, which complements the collection of very widely defined Internet connection records. The filter seems to us to be essentially a federated database and search system, very much like previous incarnations of the Communications Data Bill, the snoopers' charter or the intercept modernisation programme. It has been proposed a number of times and stopped a number of times, because of the power to look into people's lives that it would give. In a sense, that deserves an entire debate on its own, as does the recent admission of collection and use of bulk datasets.

What is a bulk dataset? Which of them have been accessed and grabbed by GCHQ so far? To whom might that apply? Just about every business in the country operates a database with personal information in it. It could be Tesco Clubcard information. It could be Experian's data about people's financial transactions. It could be banking details. It could certainly be any government database that you care to mention. From that perspective, it is hard to see where surveillance ends as a result of bulk datasets. Traditionally, we have thought of surveillance as being about communications data and as being targeted. In this Bill, we have various measures for blanket collection—bulk collection, as it is referred to—and we extend that to any private or public institution that happens to have data. From that perspective, it is pretty worrying. It is hard to see the start and end of it.

One good thing that we did not necessarily expect is that there is a thorough or, at least, a large document spelling out the apparent operational case for Internet connection records. The fact that that has been produced is a welcome step. A very important thing to do when asking for a new power is to produce documentation explaining why it might be needed. That said, it again requires examination on its own behalf, as do the GCHQ powers. They need an operational case. Parliament has not debated why GCHQ has those powers; it has merely been presented as something that is happening and that we should now legitimise. In the USA, those kinds of powers were examined—bulk data collection and use under Section 215 of the Patriot Act. An operational case was made and was reviewed by bodies that were trusted by the President and by the USA's democratic institutions—the Privacy and Civil Liberties Oversight Board and the NSA review board. Both came back and said that there was no operational case for the bulk collection and use of data; nothing the NSA had done showed that that data had prevented anything significant. That kind of review needs

to happen here. The fact that it has happened in the USA and they have come up with the conclusion that these programmes need rolling back ought to be something that you consider carefully. Parliament really needs to examine those operational cases.

Q128 The Chairman: I think that I have got the message. I am assuming that you do not think that the Bill strikes the right balance between security and privacy. Without going into detail—my colleagues will ask questions on different parts of the legislation—other than dumping it altogether, do you think that it could be improved?

Shami Chakrabarti: It could certainly be improved. One thing we would all agree on, and would agree with the Government on, is that there needed to be a new Bill, in the light of Mr Snowden's breathtaking revelations. Whether you consider him a hero or a traitor, there is no doubt that he revealed practices and capabilities where we, the people of great democracies on both sides of the Atlantic and all over the world—I would include parliamentarians in that definition of the people—had little or no idea of the sheer scale of mass surveillance that was being conducted against populations. There is a debate to be had, of course, about how much of that should or should not happen, on what basis and with what safeguards, but in the light of that there had to be new legislation, because whatever was happening was happening, at best, on very creative interpretations of outmoded laws. Some of us would suggest that it was happening outside the law and without sufficient parliamentary scrutiny, public discourse and legal authority.

We certainly agree that there must be a new Bill; there must be something like this Bill. My fundamental objection is that too much of it is about sanctioning mass surveillance of entire populations and departing from traditional democratic norms of targeted, suspicion-based surveillance, for limited purposes. There are insufficient safeguards against abuse. For example, there is the argument that I know you have had extensively about the role of the judiciary. Our position is clear. This is not a system of judicial warrantry. This is Secretary of State warrantry, save in one of the most chilling provisions of the Bill, which is about hacking and the new concept in public understanding of what the authorities propose to do. We think that is one of the gravest powers, because potentially it leaves long-term damage to systems, individuals, devices and security, after a perhaps justifiable investigation. That has the lowest safeguard of all, because in certain circumstances it involves not even the Secretary of State but, for example, a chief constable. There is too much surveillance, there are too many people, it is not to a tight enough threshold or a high enough standard and there is insufficient authorisation by the independent judiciary.

Caroline Wilson Palow: Following on from that and your introduction to the question, security and privacy are not necessarily mutually exclusive. The hacking provision, in particular, shows that there is a lot of potential to undermine security by allowing that power, including the fact that the use of malware—the type of software that allows access to computers through hacking—is not necessarily well controlled. It is like breaking a lock on a door and leaving the lock broken, so that other people can potentially get in and access the same device or equipment that was targeted in the first place. That is an example, within equipment interference, of some of the security problems. There are also greater, overarching concerns about undermining things like encryption standards and whether or not that would be permissible, both under the hacking provision and under some of the provisions, like Clause 189, which say specifically that the removal of electronic protection could be required of service providers that are subject to compliance with warrants and

authorisations under the Bill. Finally, data retention in and of itself has certain security concerns. Of course, as we have recently seen with TalkTalk here or even the Office of Personnel Management in the US, there are breaches. When you are mandating companies or even Governments to keep more information, it makes the breach even worse when it happens.

Renate Samson: I support the points that have been made about concerns with regard to safeguards. Caroline made the point that privacy and security are two sides of the same coin. We also have to look at the idea of protection. Part of this Bill is about protecting the public, yet, as has been pointed out, there are other elements that will potentially make the public vulnerable, whether that is through equipment interference or through weakening of encryption, for example. We have to step back and have a think about what protections the public require with regard to the proposals in the Bill. The idea of full independent judicial authorisation is something that I know you have been discussing at length. I would support the view that it needs to be explored in a lot of detail. We are on the cusp of being complete digital citizens. We do not have a choice any longer about our engagement online. Proposals that suggest that online engagement can be surveilled at any time, potentially, and retained for a number of months are a worry to us all. It is not the case that the Bill should be scrapped, but there are certainly areas that need to be strengthened greatly.

Suella Fernandes: On the flipside of those comments, do you equally accept that the scale and nature of the threat that we currently face is unprecedented and severe?

Shami Chakrabarti: I do not doubt that the world faces enormous threats from crime, terrorism and so on. I do not think that any of us doubts that. The question is how best to counter those threats. I will repeat the previous remarks, which are really important. It is not about a trade-off between privacy and security. A lot of what we are concerned about is actually security. What is national security if not the personal and, increasingly, the personal cybersecurity in relation to where I am—whether somebody is in my house, engaging online, and whether I am away and, therefore, open to an attack or a burglary? My financial records and so on are part of my personal security and cybersecurity. National security is to some extent the combined personal and cybersecurity of millions of people. We think that up to 50 billion emails are intercepted every day by UK authorities. There are only 7 billion people in the world, and only 3 billion of them currently have access to this kind of technology. To me, that in itself is a threat to personal security—not because the authorities are malign, but because when you collect data and create vulnerabilities, that data can be attacked by non-governmental sources and the vulnerabilities that have been created can be attacked similarly.

Suella Fernandes: On the vulnerabilities you talk about, you point out the scale of, for example, communications data and equipment interference and interception, but those powers have been absolutely essential and critical to successful convictions for large-scale child sexual exploitation, human trafficking and serious and organised fraud and crime. Those are powers that are currently exercisable by our law enforcement services. The Bill represents a drawing together and consolidation of existing powers.

Jim Killock: We are talking about several different things here. There are policing powers, there are data retention powers and there is extension of those for the police in the ICRs and the filter, so you have that body. Then you have the other area around GCHQ—what it does and how it gathers information. You have to look at both of those quite separately.

You are really asking about the operational case. As I said, my problem with the operational case is that it has not been presented to anybody for GCHQ. When the equivalent was done in the USA, the President of the USA and its democratic institutions decided that there was not really a case for a lot of it and decided to roll it back, because it was essentially purposeless. Here we have an operational case for the police with regard to ICRs, but we do not have the mechanisms, because we do not have a civil liberties board in the UK. It has not been constituted, despite potentially being put into law. That has not been examined.

On data retention in general, we have had a ratcheting back of data retention in a lot of Europe. These apparently essential tools have not been operational for a long time in Germany, the Czech Republic, Slovakia and a number of other places. There are about six or seven countries where these sorts of programmes have essentially been cancelled. There has not been a concomitant outcry from the police that they are no longer able to solve crimes and that there is spiralling dysfunction in the police. That has not occurred. Something to bear in mind is that there are often several routes to solving crimes. Data, through data retention or collection, is only one. That data probably resides on laptops and mobile phones. It will reside at service providers. That is talking only about the data side of it; there will be other kinds of factors in the equation. It would be interesting to hear from Caroline about data preservation and the standards elsewhere.

Caroline Wilson Palow: The US, for instance, does not have a data retention provision, yet it is still able to solve crimes. In fact, it uses mechanisms like data preservation orders, which are much more targeted, are not across the board and can be quite effective. You also have instances, which have been mentioned, of places like Germany, the Czech Republic and other countries in Europe where data retention is either much more circumscribed or non-existent. Again, we have not seen a collapse due to the fact that it is not there.

To pick up another point you asked about—the existing powers, particularly in the context of equipment interference—it is true that it was revealed earlier this year that the intelligence services were engaging in hacking and, when this Bill was introduced, that law enforcement, too, was engaged in hacking. Until that point, that had not been revealed publicly. The reliance on the Intelligence Services Act and the Police Act, which are incredibly broad powers, to say that that was already in statute is inappropriate, because they are so broad. There was no indication that it was actually happening. Since those Acts are from 1994 and 1997, if there was an indication in the Acts that hacking was possible, why was there concern not to reveal it sooner? Why was the position of the Government until earlier this year neither to confirm nor to deny that those powers were being used? While they may have been in use, they have not actually been in law up to this point. That is why we talk about them as new powers in this Bill.

Shami Chakrabarti: I have one further small point on comparative practice around the world and the importance of law enforcement. There is still no provision for intercept

evidence to be admissible in criminal proceedings. There has been and is to be all this interception, for laudable criminal justice purposes—public protection and law enforcement—but there is still not the provision, for which some of us have asked for many years, for interception, when it is proportionately and lawfully gained, to be used in criminal prosecutions, as is the case all over the democratic world and among our allies.

The Chairman: Thank you. I move to Dr Murrison.

Q129 Dr Andrew Murrison: I am getting the sense that you are not convinced that the "double-lock" provision, about which much has been spoken in recent weeks and on which much store has been put by those who have been involved in bringing the Bill to the position it is currently at, is really much cop. However, I believe that it is likely to remain a feature. Given that it is likely, what do you think could be done to improve the double lock? Would you see virtue, for example, in distinguishing national security from serious crime, having the double lock apply to national security and having judicial authorisation only for serious crime? Would you see virtue in, for example, a different means of appointing the information commissioners who will be involved in this process?

Shami Chakrabarti: Some of my colleagues are the great technologists and experts. I am just a humble lawyer in recovery—or in remission—so I find it easier to make the analogy with the real world when I am dealing with the virtual one. We are digital citizens, but we are still people and citizens. If I want to search your house or your office for laudable reasons, I go to a magistrate for a warrant. I can understand the argument coming from the Government that when we are doing this national security stuff and, perhaps, spying on foreign Governments, we cannot just go to any old magistrate. There has to be a double lock, surely, on something as serious as interfering with the German Chancellor's communications. That is such a political decision that there ought to be some Executive involvement. The double lock is simple: have a provision across the board for judicial warrantry, but as an internal administrative matter, make sure that those warrants are not sought by the authorities unless they have been to the Home Secretary first. In the non-crime cases—the international relations/national security cases—as a matter of good public administration, go to a Secretary of State first, but always have the sign-off to protect people's rights and freedoms, whether in the UK or around the world. Have that sign-off by a judge, as you would for your home, your flat or your office. Again, that is the practice across the democratic world.

Renate Samson: I second that. A large part of what we find ourselves doing when it comes to the digital world is incomprehensible to most of us, because it is invisible, yet we all understand what happens when somebody knocks at our door and asks to have a look around because they suspect us of something, and that element of being suspected of something is important. The real world understands a judge signing off on something. The general public have confidence that there is independence to it. While we may currently have a benign Government, we do not know what the future holds. This piece of legislation should hold up for many years. We do not know what the future will bring, so independence is hugely important. That will also mean how the judges are appointed. To feel genuinely that surveillance conducted upon us is being assessed independently and with no interference from anywhere else will reassure the general public that, should the

rest of the provisions in the Bill become law, they will be secure and thoroughly thought through, not just signed off with a flick of a Minister's pen.

The Chairman: It is said that a Secretary of State is ultimately accountable to Parliament for his or her actions, whereas a judge is not. What is your view on that?

Renate Samson: You took evidence at the beginning of this week from Mr Paterson and Lord Blunkett. I think that they answered that question for you, in that neither of them has ever stood up in Parliament and talked about a warrant they have been involved in signing off.

Jim Killock: It is also worth reminding ourselves how we got here, in a sense. The Regulation of Investigatory Powers Act had powers for the collection of material from persons overseas. The meaning of that warrantry system was extended through practice to mean every communication passing between the UK and the USA. That is how the Tempora system of bulk collection was created—through those warrants, which were politically authorised. There was a political decision, alone, to extend the meaning of those RIPA warrants, which meant that essentially Parliament was cut out of the decision, right or wrong, to engage in the programmes of bulk collection of data that we are now authorising in this Bill. It seems to me that if one is to restrain the Executive from creative interpretations of the statutes, as Shami said, you need that judicial authorisation. They should be saying, "Minister, I do not think that this is necessarily how the system was designed to work. Perhaps you might like to consult Parliament". That is a far more likely outcome than the Home Secretary saying to GCHQ, "No, I am going to deny you those powers for one or two years while I work out a political opportunity to legislate".

Caroline Wilson Palow: In conjunction with that point, it means that the judicial commissioners need the full ability to assess the warrants when they come to them. It should not be just a judicial review standard. They need to assess fully the substance of the warrant and, among other things, whether there are other less obtrusive means by which this information could be obtained. That is an easy edit to the Bill. Every time the judicial review provisions appear—it is at subsection (2) of most of those clauses—you just delete it. You take it out.

Suella Fernandes: Are you saying that the double lock and the judicial involvement strike the right balance in having judicial review as an element of the decision-making process, or are you saying that it should not be there?

Shami Chakrabarti: Judicial review does not help at all in this context. When you are deciding whether it is proportionate to issue a warrant for intrusive surveillance of an individual, let alone of a whole group of people, that is a judgment made on the evidence. A judicial review test only second-guesses the Secretary of State, in very limited circumstances. Did they make a bonkers decision that no reasonable Secretary of State could take? That is not judicial warrantry. In the statute there should be a one-stage test: the judge signs the warrant. However, because people are concerned about cases of interception on foreign powers, for example, which is classically a matter for the Executive rather than for independent judges, police officers or whatever, interception and so on of foreign statesmen and powers should go to the Home Secretary first, as a matter of good

public administration. You would not even need that in the statute, or you could put it in the statute for that category of case.

Renate Samson: Your question is interesting. I have listened to a number of the sessions of evidence that you have taken. You have all posed the question a number of times, "What exactly is meant by judicial review?". Witnesses have given you a variety of versions of what judicial review means. There is lack of clarity.

Suella Fernandes: That is exactly what I was going to raise in my question. You will agree that, with judicial review, the judge would have access to the same information as the Secretary of State or the Minister.

Shami Chakrabarti: I do not think that is suggested in the Bill. There is nothing to suggest that.

Suella Fernandes: That is what judicial review involves, does it not?

Shami Chakrabarti: No, it does not. This is a term of art. A judicial review test, as a matter of our law, is a very limited opportunity for a judge to second-guess a decision that has been made by a public authority, whether it is a Secretary of State, local government or whatever. It is not a double lock.

Jim Killock: Basically, it is, "How did you follow procedure?", is it not?

Shami Chakrabarti: Yes. Did you make a decision that was within the realms of a reasonable decision? Could any reasonable Secretary of State possibly have made that decision? It is not appropriate for warrantry.

Suella Fernandes: What about the proportionality test, which involves balancing the right infringed and the objective met? That goes further than what you are suggesting, does it not?

Shami Chakrabarti: But that has not been allowed to the judge, under the provisions of the Bill. They are not second-guessing the Home Secretary's decision on the merits of proportionality, under the Bill.

Caroline Wilson Palow: That is exactly our concern. When you talk about judicial review, all you are doing is looking to see whether proportionality has been assessed by the Secretary of State. The judge will not have the power to say, "You have made that assessment incorrectly". In the US, to give an example of a comparison between two different types of warrantry there, a normal warrant would go directly to the judge. There is a political consideration that is made ahead of time. For instance, the US attorneys, who are the federal attorneys who often start the process, are politically appointed and will make a decision about whether or not to seek a warrant in the first place. Once that is done, it goes directly to the judge.

Suella Fernandes: Before we finish this line of questioning—I know that other people want to get in—I need to put on the record that the statute states explicitly that it must be "proportionate" and "necessary". That is the relevant test.

Shami Chakrabarti: You have to look at Clause 19(2).

Caroline Wilson Palow: The concern is the way in which the two play together. That is why I said that we think you should just delete subsection (2). We totally agree that necessity and proportionality need to be assessed, but, once subsection (2) is in there, it reduces the ability of the judicial commissioners to make that assessment. To continue the parallel that I was trying to draw, in the US there has been a lot of talk about the FIS Court, which acts on foreign intelligence. This is PRISM—the types of authorisations for collecting intelligence on people around the world. Its powers are the equivalent of what judicial review would be here. Essentially, when a request comes to it, it has to check the box to say that everything has been considered as necessary, but it does not necessarily get to question the conclusions that were reached by the person who was seeking the warrant in the first place.

Shami Chakrabarti: A double lock would mean, "I can substitute my decision on the merits for yours". Traditional judicial review means, "I look at the way you made your decision, but I do not substitute my own for yours". You have to be procedurally irregular or to have made a completely insane decision that no Secretary of State could make. That is achieved by Clause 19(2), otherwise there would be no purpose to it.

Matt Warman: We have had an awful lot of witnesses tell us that their expectation and understanding of what the Bill says regarding judicial review would, as Suella Fernandes has said, in fact mean a test that looked at the evidence. It would have to be proportionate and go through all those things. You are saying simply that that is not your understanding of judicial review. It therefore seems to me that we are talking simply about definitions; we are not actually talking about a principle, because what we have been told is what you are saying you are asking for.

Shami Chakrabarti: It just does not stand up in law. These are well-tested terms. If you want to create a full merits appeal in statute, there are many precedents for doing that. You do not put in a clause like 19(2); you can do it much more simply. I believe that you will hear from the Secretary of State in the not-too-distant future. You can just ask her: "Is it your view that you will make an initial decision and there will be a full merits review? The judge can just second-guess your decision and make a different one. Is that your intention?". If she says that that is her intention, that will help for Pepper v Hart purposes, but there are far clearer ways to deal with it, like just deleting Clause 19(2).

The Chairman: Thank you. Can I move to Mr McDonald?

Q130 Stuart C McDonald: I have another million-dollar question. What is your understanding of the meaning of the term "Internet connection record"? Why would their gathering and analysis be more intrusive than for other forms of communications data?

Shami Chakrabarti: This has been quite a journey for me. I have had lots of younger and more technologically savvy colleagues explain the sheer scale of what we might be looking at as regards Internet connection records. If you take your favourite device—your smartphone, your tablet or just the sites you go to from your laptop or desktop—we are looking at things like the websites you visit. We are looking at the communications software that you might use to speak to your mother—Skype, WhatsApp and so on. We are looking at all the icons on your menu, such as your Twitter and your diary. Recently a health one popped up on my phone uninvited, telling me how many steps I took yesterday. Taxis,

maps; the list goes on. Photos, my Internet shopping, banking apps—I understand that all those things are potentially within the broad concept of Internet connection records. As we look just a little way into the future, in the discussion that people describe of the Internet of things, more and more of our real lives will be managed online. Now we will be talking more and more about the little icons on our devices that connect to our fridges, our cars, our burglar alarms, our gaming devices and so on, so the separation between my real-world security and privacy and my cybersecurity and privacy is almost completely collapsed. This is very intrusive on millions and millions of, for the most part, completely innocent people.

Renate Samson: It comes back to the point that I made that we are all now digital citizens. It is that—it is life. It may feel at the moment that it is just a mobile phone and a laptop, but, as Shami explained, with the Internet of things it will be everything. That will create a huge amount of data that will be constantly ticking over. We have been informed that the Internet connection records are just the URL, before the first slash, of a website and no content, but from the technical evidence I have been listening to and you have been receiving, and from all the different things that I have read, which Jim will probably be able to explain better, I am not entirely sure that it is quite as clear-cut as has been implied. I would certainly like to hear from the Home Office—from government—with regard to this Bill a very clear definition that it knows exactly how this can be done, because I am not sure that I do.

Jim Killock: It seems to me that essentially the Internet connection record starts from the point of view that the Home Office wants the power to have retained the fact of somebody using the Internet, with some other service, and to record that. It has decided that the best way to do that, given how much the Internet is used, the purposes it might be put to in the future and the services that might appear, is just to say, "Let's have a very broad definition of anything that connects to anything, whether it is a person or a machine. That will allow us to compel Internet service providers to collect information about anything we deem important in the future".

I do not think that is really a good way to legislate. It is incredibly broad, it is open to abuse and the cost implications are impossible to put a number on. If you have power to collect and retain any information, no matter how difficult that is and how much of it there is, essentially you have just written a blank cheque to scale up surveillance indefinitely. Of course, once you have an initial investment and the thing has started to roll out, that poses the problem of how you restrain it in the future when it turns out to be not quite as useful as you hoped. Do you pour in another few tens of millions of pounds to extend the amount of information that you are collecting under this very broad power? Given that the companies will probably tell the Government that it will be more effective if they spend that extra bit of money, this seems to be a financially haphazard way of working, as well as haphazard in terms of human rights and the proportionality of the surveillance we are authorising.

Caroline Wilson Palow: This is quite a confusing definition, because essentially you have two different definitions in the Bill. You have Part 3, where Internet connection records are explicitly mentioned, but in Part 4, under data retention, you have a clause that, under the commentary, is supposed also to encompass Internet connection records. The definitions

do not completely align, and for that reason we are somewhat confused about what Internet connection records really are.

Let us take an example from the commentary that Renate has already mentioned—the idea of taking the domain name of a website, which is the information before the first slash. Potentially, that could be quite intrusive and could reveal a whole lot of information. It is not as innocuous as just bbc.co.uk, which is the example that they gave. For instance, that domain name could be saveyourmarriagelikeme.net or domesticviolenceservices.com. Maybe one of the most interesting ones is crimestoppers-uk.org. This is where you can make anonymous tips to help to solve crimes. Of course, if you had the Internet connection record that said that someone had gone to crimestoppers-uk.org and you also knew the time when the tip had come in—if you were the police, for instance—you could very easily figure out who had put in that tip. That is a real problem, because if you are destroying that anonymity you can undermine the ability to solve crime.

Q131 Mr David Hanson: This is the central question many of us will have to wrestle with. Surely the police, the security services or whoever accesses that, under authority, with judicial review, is doing so only because there is some potential link to a potential investigation. The vast majority of people will never have that link checked or looked at. I am wrestling with that myself. I want to get your assessment of whether the proportionality is there. If we do not collect the information, none of those leads can be followed up.

Shami Chakrabarti: You are collecting huge amounts of sensitive information that is not currently collected and, therefore, you are creating the vulnerability I am so concerned about. I am not even talking at the moment about potential abuses by the authorities. I am talking about the vulnerability to hacking by other people that you create when you create a massive sensitive database and put the entire population's online life under surveillance in this way.

Renate Samson: My understanding is that this would help to support requests that are already made for communications data. At the end of November, IOCCO published as a starting point to a further publication a breakdown of 100,000 communications data requests by 29 police authorities, including the National Crime Agency; 46% of those requests related to burglary, robbery, theft and drug offences. If this is to support that, people may see it very much as an intrusion. On that sort of issue of crime, why do you need to know what website somebody has looked at with regard to burglary? We have to think about the intrusion into people's lives, based on us as digital citizens, before we start to discuss the retention and use of Internet connection records. Their retention is an issue I know you have looked at, but off the back of the TalkTalk hack, for example, we need a lot more clarity on how companies will be asked to store that data to ensure that they are safe.

Jim Killock: You also have to consider the wider effects on society. If I said to you, "When you go home, can you note when you got home and which newspaper you read, although do not worry which article it was? If you ring your family this evening, make a note of that and then tomorrow, hand it into the police", you would think that an excessive ask.

Shami Chakrabarti: And every hotelier, every restaurant owner, every pub, every cinema and every theatre that you enter will be required to keep a record of when and where you entered. That is the equivalent of what is being proposed.

Jim Killock: The question then is, is that a proportionate thing? What are we trying to solve? Is it quite as desperate a situation as is being claimed? As I said, these powers do not exist in other democratic countries. Russia has just been given a bit of a rap for similar sorts of activity. A number of European countries have rolled back on traditional data retention, never mind this kind of extension.

The Chairman: Lord Strasburger?

Lord Strasburger: My point has just been covered.

Q132 **Stuart C McDonald:** Are there other ways to go about IP resolution that are less troubling? The Home Office and law enforcement agencies will say that retention of these connection records is essential for that to be successful.

Jim Killock: One thing that you have to ask is whether the technology will out-evolve this. Will IPv6 catch up with some of the problems that it is currently seeing? You also have to ask how the Internet might work in the future and whether any of this will work. Some of the evidence that has been put about is quite interesting. People have said, "How do we know whether somebody has used Twitter or Facebook? We need to know in emergencies whether somebody has been accessing that website". Phones just do that now every couple of minutes. If they are constantly connecting to all these services, you will just have a huge glut of information that is not a fat lot of use to anybody.

Q133 **Matt Warman:** One of my frustrations with this conversation is that it is always said that the Government are being asked to hold this stuff. Actually, we are asking ISPs to hold it. That is a very important distinction that we need to continue to make. Law enforcement agencies tell us that they want access to the information and are happy for it to be held externally. You seem to be saying that you are not happy with that. I wonder what alternative you would propose.

Jim Killock: It may not be a government-held database, but it is a series of data centres that are all accessible by a single mechanism that can then be queried in parallel from an officer's desk.

Matt Warman: With appropriate oversight.

Jim Killock: There are some interesting things there. It seems that the way it will work is that you can get an officer to ask the computer whether it has any useful information in a case. It will tell you the things that it might have, and then you can go off and get some warrantry for it. It is almost saying, "We will go not on fishing expeditions, but if you did, here are the results you would get. Why don't you have a think about whether or not that is useful?".

Renate Samson: You say that there will be appropriate oversight. Currently the Bill will retain the process that we have now. From Big Brother Watch's point of view, that is not

appropriate oversight. We would like to see a further layer of independent judicial approval and authorisation of an internally signed-off warrant.

Matt Warman: The point I was making is that it is not a free bucket any policeman can look at.

Renate Samson: We also have to acknowledge the recent case with regard to Police Scotland and on which IOCCO reported, where warrants were being signed off and misused.

Matt Warman: Misused being the operative point.

Renate Samson: Yes.

Shami Chakrabarti: Sometimes that will happen. To go back to the real-world analogy, when I said that this is the online equivalent of requiring all those businesses—hoteliers, restaurants, cinemas and so on—to keep a detailed record that they do not currently keep of everybody's comings and goings, that does not mean that I am against ever putting a particular hotel, restaurant, gym or whatever under surveillance. I just think that you take a targeted approach. When you get suspicion that conspiracies are being conducted in a particular room above a particular pub, at that point you put that site under surveillance. Then you put the people who have been to that site under surveillance. That is the kind of approach we should continue with in our democracy, in the virtual world as well as the real one. If you have concerns about particular activity and sites, you can go to ISPs and CSPs and ask for the data they currently hold anyway. You can seize people's devices, because those people or organisations have now come under suspicion. You can target suspicion not just around individual people but around organisations and, indeed, websites.

Renate Samson: I want to clarify your point about misuse. IOCCO is very clear that judicial approval was not obtained to acquire the communications data. My point, and the point of Big Brother Watch, is that independent oversight and authorisation of an internally signed-off warrant for communications data would, I hope, potentially ensure that misuse did not occur. That is just for clarity.

Jim Killock: The important thing is why we have the idea that necessary and proportionate surveillance is essentially targeted, rather than blanket. Why do we have that rule? Why has that been pushed forward? It is easy to imagine that in the UK we will never have any problems with our democratic institutions, the police will never overstep the mark and we can solve all this through authorisation regimes. However, if you look over the sea in France, you have the potential of a Front National Government, with parallel powers. You have powers similar to these in China and Russia. Is it the role of the UK to say that blanket surveillance, easy profiling and access to everything that everyone does in their lives is the right international standard to set and is absolutely, 100%, guaranteed never to turn into a problem in this country, or should we restrain surveillance to somewhere we can trust, for ourselves, for other people and for the long term?

The Chairman: Can I move to Lord Butler?

Q134 Lord Butler of Brockwell: I want to ask you about equipment interference. You have made reference to that. As I understand it, you are not claiming that equipment interference in the past has been non-statutory. You are claiming that, although there are statutory powers, they are very general, they have been widely interpreted and the public have not been aware of what is going on. Do I have your argument right?

Shami Chakrabarti: You do have my argument right. I do not believe that equipment interference was necessarily in the mind of the legislators when the provisions that are now being relied on were passed. Those provisions were more about traditional breaking and entering, bugging and so on. I certainly do not think that the public understood in that way the activity that was being justified ex post facto. That creates a problem for Article 8 of the convention, which requires a certain level of public understanding for something to be law for the purposes of the ECHR. Those powers were there and they were used for more traditional interferences, but hacking is a very, very serious business. It is more than just surveillance, because you are potentially changing data and causing long-term damage to data security. I am not saying that it should never be allowed, because that would be like saying that you should never break and enter in order to find the hostage, the terrorists and so on; I just think that there should be much tighter safeguards for hacking in the Bill. Again, in principle, it should be a targeted approach, not a blanket one.

Jim Killock: It is worth remembering that the hacking power has already caused some very significant problems. You probably remember that Belgacom, the telecoms provider in Belgium, was hacked by GCHQ, allegedly. In the first month of the clean-up, that cost it around £15 million. A series of telecoms providers, including Deutsche Telekom, were also hacked by GCHQ. Those are law-abiding companies. They are not terrorists. They have information and are a conduit to further information, perhaps, but they are also people who can be compelled to co-operate with their own national authorities. However, GCHQ, under this warrantry and hacking regime, has instead taken the view that foreign, legitimate companies with international stature, within the bounds of Europe where we have common laws and systems, are a legitimate target for hacking, and that the clean-up operations are, frankly, not our concern.

Lord Butler of Brockwell: Could we stay within the UK for the moment?

Jim Killock: But this is a UK operation.

Lord Butler of Brockwell: I know that it is a UK operation. I am just talking about the targets at the moment. The point that you have made is about overseas targets. That is a separate consideration. Within the UK, you must agree that it is an advance that this proposed Bill gives specific authority for and introduces transparency into that power.

Shami Chakrabarti: I agree with that. I wou*l*d just like it to be more tightly regulated, given the consequences.

Lord Butler of Brockwell: Sure. You are not arguing, are you, that such a power, properly warranted—we have had discussions about what proper warranting is—may not be a legitimate weapon?

Shami Chakrabarti: In extremis. The intrusion is graver, because it is not just surveillance but actual damage—not least, potentially, damage to fair trials, if now every criminal defence lawyer can argue, "This isn't a genuine email. This isn't genuine data any more, because of hacking capacities". Given how serious the consequences of hacking are, the thresholds possibly need to be even higher than for other powers in the Bill.

The Chairman: I will now move to Lady Browning and Lord Henley. I am conscious that there is a vote in the Commons at 7 pm, but I would very much like the Commons members to be here for the questioning.

Q135 Baroness Browning: You have all expressed concern about Clause 189. I wonder whether you could share with us what you believe the effects will be on both service providers and customers. Ms Wilson Palow, your submission stated very clearly your concern about this.

Caroline Wilson Palow: It is a very broad power, to begin with. Essentially, it says that obligations can be placed on service providers to facilitate interception, hacking or any other power in the Bill, and they would need to take those steps ahead of time, before an authorisation or warrant was placed. Within that broad power, there are some examples of what might be done. A particular concern of ours is the removal of electronic protection. We interpret that as the potential to undermine encryption. Encryption is crucial to so much of what we do all the time, including all our financial transactions. It gives us the security to operate online. The removal of encryption has the potential to undermine all of that. We think that the balance there has not been struck appropriately.

Shami Chakrabarti: Taking my real-world analogy again, because of my poor understanding of these things, I do not think that it would be proportionate to give government the authority to demand that every locksmith in the country makes a spare key every time he is setting a lock for a home, a property or whatever. It is proportionate in certain circumstances, under warrantry, for the authorities—the police—to break into a targeted property because we believe that there are explosives, contraband or evidence there. To ban privacy, to ban private conversations and to require people who live on trust—companies that are all about creating a space of trust, so that we can have trust in our banking system et cetera—to leave those gaps in the nation's cybersecurity is quite problematic.

Renate Samson: It is the point that we were making earlier. The Bill is about protecting society. Encryption enables the protection of society. It enables people to use Crimestoppers. It enables whistleblowers to lay clear things that are going on that benefit society. It enables the vulnerable to communicate safely. Battered wives, for want of a worse expression, can ensure that they communicate as necessary. People on witness protection programmes can have an element of safety. It is much broader. It involves all of business. When all the communications in our home and everything else we have talked about on the Internet of things are connected online, we all want to know that our energy can be supplied safely. Encryption, as our submission to you explains, is not just a concern of privacy campaigners. It is a concern of Governments and business and one that will impact on us all, as all our lives are lived online.

The Chairman: Thank you very much. I move now to Lord Henley, on the Wilson doctrine and other matters.

Q136 Lord Henley: There is protection in the draft Bill for legally protected communications of journalists and journalists' sources, and there are protections for Members of Parliament of both Houses, enshrining the Wilson doctrine. Do you think that the Bill goes far enough?

Shami Chakrabarti: Not at all. There is room for some serious improvement. Let me be positive: there is room for real improvement. As far as I can tell, the Wilson doctrine has been completely reneged on. Recent statements by the Prime Minister suggest that, effectively, there is no Wilson doctrine in practice any more.

Lord Henley: What particular comments of the Prime Minister are you referring to?

Shami Chakrabarti: My understanding of recent statements from the Prime Minister is that there is now no absolute practice of not intercepting parliamentarians' communications. That was an absolute promise that came from Prime Minister Wilson and, indeed, was repeated by subsequent Prime Ministers.

Lord Butler of Brockwell: No. I am sorry, but you are wrong about that.

Shami Chakrabarti: I have read the Wilson statement. As regards what could be improved, I accept that there could be certain very rare circumstances where it would be justifiable, in a democracy, to interfere with even the communications of parliamentarians, lawyers and journalists, but we want something closer to the provisions that you currently have in place for production orders. You want something approaching reasonable grounds for believing that a very serious criminal offence is happening or has happened, and that there are no alternative ways of getting to the evidence; otherwise there are real dangers. Think of the political dangers. Perhaps it was just a rhetorical flourish, but we have had leaders of parties suggest that opposition parties are a threat to national security. I do not think that it is healthy for democracy for opposition political parties to believe that it is possible that they can be intercepted just on the say-so of a political opponent, even if that political opponent is the Prime Minister.

When it comes to legal professional privilege, we now know, because of the Belhaj case, that the security agencies were looking at legally privileged material that was relevant to a case being brought against them in relation to torture. There need to be much graver safeguards—we are back to judicial warrantry—and a very strong presumption against looking at parliamentarians' communications, legally privileged communications and journalists' sources.

The Chairman: Thank you very much. I will give you just one or two more minutes, because I want to wrap up with a couple of suggestions about how you can give us more evidence.

Jim Killock: I want to say something very specific about this. It is very hard to tell where the boundary between journalist and non-journalist lies. In this day and age, it is not somebody who is working on a paper; it could be somebody writing a blog and self-publishing. Many NGOs have a similar role to journalists in exposing, commenting and publishing. Particularly with communications data, where the system sometimes has to go to a magistrate or

whatever and sometimes has to be self-authorised within the police, it breaks down when you have this blurring, which is a very strong reason why all authorisation should be done by an independent authority. That, in particular, has been spelt out in the data retention judgment by the CJEU; when communications data are accessed—in that case, it was talking about retained data—there should be independent authorisation. This is one of the reasons why.

The Chairman: Thank you very much. It has been a fascinating session. It really has—very revealing. If in the evidence that you present to us you want to go into some of the detail of any amendments or drafting issues that you feel would improve the Bill, which you mentioned earlier, please feel free to do so and send those suggestions to us. Thank you very much for coming along today.

Detective Superintendent Paul Hudson, Head of the Metropolitan Police Service Technical Unit (QQ 162-173)

Evidence heard in public Questions 162-173

Oral Evidence

Taken before the Joint Committee

on Wednesday 16 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Lord Butler of Brockwell, Bishop of Chester, Lord Strasburger.

Witness: **Detective Superintendent Paul Hudson**, Head of the Metropolitan Police Service Technical Unit, gave evidence.

Q162 **The Chairman:** A very warm welcome to all of you. I was just saying that this is a rather large room—a bit like Mussolini's waiting room, if you ever saw that. You are miles away down there. Can I say how valuable the Committee thought our visit was yesterday, by the way, as an introduction? It was extremely useful and gave us a lot of food for thought. I am going to start the first question and my colleagues will come in afterwards. Do feel free, each of you, to comment on the answers, if you so wish.

This question is very general. What is your view on the Bill? To what extent do you think it is necessary, and how will it improve and affect the operational work of your respective organisations? Do you feel it goes far enough?

> ***Michael Atkinson***: Thank you, Lord Chairman, for inviting us here today. We are pleased that yesterday was of benefit, hopefully to you all, to see how our working practices take place.
>
> Could I first introduce us? My name is Michael Atkinson. I am the secretary for the National Police Council's Data Communications Group, and I work for ACC Richard Berry, who appeared in front of you several weeks ago. To my right is Detective Superintendent Matthew Long. Matthew is a deputy head of UK operations within CEOP, which is part of the NCA. I hope that Matthew and I may be able to provide you with some evidence on our use of CD and how this relates to the Bill. On my left is Detective Superintendent Paul Hudson. Paul leads and is the head of the Metropolitan Police Service's technical surveillance unit. He will, I hope, deal with any questions you have in relation to equipment interference.

The Chairman: Thank you very much indeed. Of course, we met some of you yesterday. Anyway, what is your view of the Bill? Is it right? Is it necessary? Does it do what you want it to do, and does it go far enough for you?

Michael Atkinson: I suppose it is no good me sitting here talking to you about the change in technology. You have probably all seen enough, since you have been in this Committee, about how technology has changed. What is happening with policing? We are struggling. How are we struggling? We are struggling to keep pace with how victims, witnesses and criminals use technology. In many investigations, we try to use CD as evidence. It is causing us problems to obtain this evidence. We use CD in many investigations: theft, child sexual exploitation, homicides or frauds—a wide spectrum of offences. Our inability to obtain this data is increasing, for various reasons. Some CSPs do not retain the data for long enough in certain services. Some CSPs are outside our jurisdiction; we have difficulty with their laws in obtaining the data, and some CSPs outside our jurisdiction will not assist us. Also, some of the data is not retained. I have said that it is not retained for long enough, but the actual data that we require is not retained. We believe that this Bill will assist in closing some, but not all, of the gap that we are currently experiencing.

Paul Hudson: Lord Chairman, if I may I will also bring you the EI perspective on this. We would seek further capability. The Bill currently provides extra oversight, which we welcome, but it is all about serious crime. On very rare occasions, as I hope we demonstrated yesterday, we might use EI to protect the most vulnerable people, and that might not be in serious crime; it might be to save them from doing harm to themselves. So, in the emergency provision, we would look for something that legitimises that use of EI: to protect the most vulnerable people from harm.

Q163 Mr Hanson: Thanks for coming in. My apologies for yesterday; I was on another Select Committee elsewhere in the building. For my benefit, but also to put it on the record, it would be really useful if you could give a couple of concrete examples of how the current use of powers has led to convictions or, as you have said, has been of help in providing safety or rescue to individuals.

Michael Atkinson: Unfortunately, you were not there yesterday, because you would have been provided with evidence that clearly showed how we use communications data in protecting the vulnerable. You would have seen and had explained various examples of young missing children and people who were going to commit suicide. Unfortunately, we did not manage to save everybody.

We use the vast majority of communications data to protect the vulnerable and save people's lives. In addition to that, our use is predominantly in two areas of our business: proactive and reactive investigations. That is what we use communications data for. In proactive investigations, we may use it to identify a conspiracy and people talking to each other. We may use it to identify people's whereabouts at certain times. We also use it to identify other leads; for example, somebody may have phoned a travel agent and it gives us a lead so that we can go there. We may be able to get that information, take further steps and make further inquiries. So in proactive investigations, we use it in various ways.

In reactive investigations, the offence has predominantly taken place. Murder is probably one of the more serious crimes that we look at. My background is as an SIO, and in every murder investigation in which I have been involved we have used communications data. Why do we use it? We need to identify where the victim was and where their last movements were. It may be over a 24-hour period or it may be just a relevant period of time. We also look at and identify people with whom they have had contact and, again,

that may be over a 24-hour period or a specific time period. That is no different when we identify a suspect: we would look at their data, their locations and who they are talking to. We use it across various offences.

We use data together with forensics and other data opportunities, such as ANPR and CCTV. In 2012, we undertook some work and identified communications data use in 95% of all serious crime prosecutions. We use communications data in 100% of counterterrorist investigations. Matt will probably give you some more examples of how it is used in CEOP and its work.

Matt Long: In answer to your question, the Bill is essential and invaluable. I will give you two operational examples. First, the National Crime Agency's CEOP receives between 1,300 and 1,500 referrals every month from the National Center for Missing & Exploited Children in the US, the majority of which are reported online. Every one of those is a child at risk or a suspect for us to identify, and with the majority the starting point is the communications data. For each of those, myriad further victims or suspects may be identified who we need to follow, so in the daily, weekly and monthly movement in the National Crime Agency that is the volume that we need communication data to support.

A more personal example is that I am still the senior investigating officer for Operation Notarise. Within that operation, we arrested 745 offenders nationally. Every single one of those offenders who we arrested had a comms data application attached to them, and some had multiple applications. Within that investigation, we safeguarded over 518 children, so as the senior investigating officer I see it as a tool in the toolbox, although not the only tool; it is complemented by other tools such as open source. To summarise, there is that daily, weekly protection of children. In the large-scale and small-scale operations, we need it critically to progress.

Mr Hanson: What areas of new media are you not able to access now because of the way in which the legislation is currently framed?

Matt Long: A very simple example, which I was going to come on to later but will bring in now, because it illustrates it, is in grooming. With the grooming of a child on a communications platform that is online only, if we request that data we want to know who that child is talking to. Who is that offender? Are they talking to other offenders or children? There is some data that we simply cannot get. If that is the only route by which they are communicating, which is increasingly the case, it simply is not available to us.

Mr Hanson: What is the difference between seizing PCs and seizing mobile telephones to get that data, as opposed to having the powers under this Bill?

Matt Long: You need to have the computer or the phone to be able to do it in the first place. Our difficulty is that we may have a report that has come across from the National Center for Missing & Exploited Children, which says that a child is in communication with an individual, and we do not know where they are and do not have the devices. It is quite easy once you have the offender in custody and you can go to the device. Then we will proportionally assess those devices and see how many offenders we can identify and other routes that we can follow. Ultimately, sometimes the very first step is that communications data. Without it, we cannot take the first step, which is the identification.

Q164 Lord Strasburger: Good afternoon, gentlemen. Is accessing internet connection records, if that can be done, essential for the purposes of IP address resolution and identifying persons of interest?

Michael Atkinson: I have spent several hours in one of the UK CSPs for mobile phones. I cannot sit here and say that I am a technical person who understands the technical issues to do with how telephones are used, how they retain the data, what data they retain and what they might need to do to provide ICRs. What I can say is that they are assuring me that, without the retention of ICRs, they will not be able to solve internet protocol resolutions. They also tell me that we will not get the evidence that we need in order to undertake further investigations of people who may be of interest to us. Matt has given you one example. Another example is a terrorist investigation. We do not do live inception in all terrorist investigations that we undertake. We may do investigations for months and months, identifying intelligence, connections between people and what the suspects are intending to do. If we are investigating some suspects and have some intelligence but it is insufficient to arrest, we would like to know whether they have gone to a website on how to make a bomb, whether they have gone to a website of a major shopping place in the UK, whether they have gone to a website where they might wish to book some tickets to leave the country. Currently, we cannot get that. We believe, and we are told by the communication service providers, that ICR will solve this.

Q165 Shabana Mahmood: Last week we had oral evidence from a number of smaller CSPs, and one of the things they said on internet connection records that struck me as important was that the internet connection record would probably provide a useless bit of information. If you had a mobile telephone for a young missing child, for example, all the ICR could tell you is that that phone had been connected to Twitter or Facebook for 24 hours a day for the last six months from the point at which the phone was bought, because many of the apps that are used are automatically connected to the internet. I have just checked my phone. I have background app refresh on, which means that it is automatically connected on a 24-hour basis. Is there a danger that lots of information that you collect from internet connection records is just useless: it gives you no additional investigative assistance?

Michael Atkinson: Again, we look at what we are being told by the largest CSPs. If we have a missing person, we conduct a lot of inquiries. CD may not be our first inquiry. We have other inquiries to undertake, but we may identify that the missing person has a phone. What better way to trace them than through the cell site to identify where they are?

Sometimes phones have been turned off, but we can get back the fact that they have been talking on Twitter to somebody. Even just by getting that back, we can go to Twitter. Twitter, and not necessarily just that company but other companies, will help us to identify vulnerable missing people. They will identify to us that they may have been in contact with certain people, who would give us further lines of inquiry and may allow us to identify where this missing person is. ICR could tell us that they have booked a train ticket. They have gone to a train line; it looks as though they have booked a train ticket. We can make inquiries with them. We can see that they have. Maybe we can locate where they have gone. The CSPs that I have spoken to have made it clear that ICRs would assist us.

Shabana Mahmood: National Rail Enquiries, which is the main app that most people use for booking their train ticket, is on 24-hour background app refresh. I suppose this Bill is

introducing a whole new regime for internet connection records. My question is: is it necessary? Will it just give you oodles and oodles of useless information? If you are trying to trace a child, you know they are on Twitter and you can get into their Twitter account or ask their friends, who are more likely to be able to tell you what the Twitter or Facebook activity of that young person was.

Michael Atkinson: That is what we try to do, but there is always this issue. Matthew explained the relationship with grooming. We can get a lot of information that can assist us to identify where they are. We realise that there is collateral intrusion. We realise that there are risks to this, but on the other hand there are children and missing people. Are we willing to go further to try to save a life or to bring the person back to their family?

Stuart C McDonald: First of all, just following up on those points, in quite a lot of missing persons cases, for example, it must be pretty straightforward to establish whether the missing person has a Twitter or Facebook account and then, once you have done that, you can go to these communications service providers and find information about who they have been contacting and so on.

Michael Atkinson: Sometimes we can, yes.

Stuart C McDonald: How often are you frustrated in trying to find what people have been doing to communicate with others?

Michael Atkinson: I cannot sit here and say how often it happens. What I can say is that it does happen. Some companies will not assist us; some companies that are outside our jurisdiction will not support us and help us with identification, but many of them do.

Q166 Stuart C McDonald: Now, as you will understand, the proposal is for communication service providers to be required to retain communications data and internet connection records for 12 months. What is your comment on 12 months being the specific limit? Would you want more than that, or could you cope with six months or three months?

Michael Atkinson: It is interesting that this has come up several times. I was involved in the 2012 Bill. In 2012, we undertook a survey across policing. Sixty-four law enforcement organisations, in 2012, undertook applications for communications data. We received replies from 63 organisations. They undertook a two-week survey in every SPOC unit. The unit that you went into yesterday recorded, over a two-week period, every application that went through the unit in each of the 63 organisations. That gave us a really good breakdown of how we use communications data, but also of the history of the data that we are applying for. To give you an example, we covered nearly 10,000 pieces of data and applications. That is what this survey was about. Nine per cent of those applications were for sexual offences. What was interesting was that 37% of that 9% of data that we applied for was more than six months old. We would say, and you can see, that retaining the data for more than six months is very important. We also identified that 1% of all the data was for terrorist investigations, and 27% of that data was more than six months old. Now, I know we are writing to you, Lord Chairman, and we would be happy to provide that data to you with our submission, but it provided us with some really good background and understanding of why. Further, it shows what is more than nine months old or 12 months old, so there is more data there.

What is really interesting is a document produced by IOCCO on 20 November, only last month, which is a breakdown of communications data and applications. It shows over 100,000 communications data applications, 19% of which were in relation to sexual offences. Two things jumped straight out at me. First, this is a 100% increase from the survey that we did in 2012. Secondly, 37% of roughly 19,000 is over 7,000. We would say that, if we retain data for only six months, hundreds if not thousands of suspects for sexual offences would likely evade prosecution.

Stuart C McDonald: Can I just pick you up on that, though? That information is very useful, but it does not tell us how crucial that information is at six months old, 12 months old or whatever it is. I suspect it is almost impossible to gather that, but what is your personal view?

Michael Atkinson: We have had the conversation about when we undertake investigations. A homicide investigation is a bit like a jigsaw, but you need all the pieces to make the picture. I will have communications data. I may have CCTV. I may have forensic data. I may have ANPR. There are quite a few pieces to make up that jigsaw. What you cannot necessarily say is which piece was crucial in detecting and prosecuting that person for that offence. The whole picture helps to prosecute, not an individual piece.

Q167 Victoria Atkins: Following on from that, perhaps this is an easier way of looking at it. Is there a single serious organisation case that you have investigated and taken to trial in the last decade that has not involved mobile phone records or records of telephone communications?

Michael Atkinson: I cannot sit here, hand on heart, and say 100% that there is, but the data shows that in 2012 we used it for 95% of all serious and organised crimes. I would be very surprised if any serious and organised crime case went to court where we had not used communications data.

Matt Long: Perhaps I could elaborate further for you. I gave the example earlier of Operation Notarise, with 745 arrests and 518 children safeguarded. In that operation, within a 12-month period, we resolved 92% of data. If I had 12 months, I would get a 92% return. If that dropped to six months, I would lose six out of 10 of the pieces of data. Out of six months, we would lose 60% of that offending population. If you dropped it by a further 12 weeks, I would have lost 87% of the lines of inquiry presented to me. In that case, the first point was communication data. To answer your question about what the impact would have been on me in that operation, it would have been those percentages at those time stamps. When you think about that in relation to that operation, the majority of the offenders in that operation were not known to law enforcement. It is not as though I have another database that I can check and then identify that person by some other means. I simply cannot do that. When you think that 15% of those people were in a position of trust—they were a teacher, a scoutmaster or in another position where they were the guardians of our children—it is very unlikely that I will find another route, because those individuals have gone through criminal record checks. They have gone through the very good safeguards that we have as a country, but effectively they have beaten them. That example shows you what the output and the outcome would be if you reduced the length of retention in those ways.

Michael Atkinson: Sorry, Lord Chairman, could I just cover one other point? We do not use communications data just to prosecute people. We clearly use it also to prove that people have not committed an offence. The defence uses communications data. For our more serious cases, especially if we are talking about counterterrorism, homicides and serious and organised crime, can take six months, nine months or over a year to come to trial. If the defence serves their defence statement on us six or seven months after the offence has taken place and we only retain data for six months, it would prevent them from having a fair trial and it would prevent us from checking alibis and defence statements, so we believe that 12 months is the appropriate period.

Matt Long: Can I make one final point on that? The other thing, going back to your point, is that victims do not disclose on day one when the communications data is available to us. It may take them weeks or months to gain the confidence to disclose. Then, we do not get a consequential order of victims so that we know that A leads to B who leads to C. It might be that A leads to E, E leads to another 100, and we have to review them. All that takes time. It is not necessarily even at that first instance of the offence when we need the data. We need to conduct the investigation and be allowed sufficient time to do that. Sometimes that can take months.

Q168 **Dr Andrew Murrison:** Good afternoon, gentlemen. Twenty years ago, we did not have any of this technology available to us, so setting aside crimes that are specific to modern communications such as online paedophilia et cetera, it follows from what you have said that since you now do have access to all these investigative modalities, your clear-up rate should have been dramatically improved and your ability to secure missing people, for example, should have been improved. Is that in fact the case?

Paul Hudson: As much as we have greater technological investigative powers, the criminals we seek to arrest and bring before the courts also have greater technological ability to avoid us. We have seen that the increase in technology, the mobile nature of communication and the mobile nature of making meetings have made it more difficult. The criminal of 20 years ago used to meet at a safe house and it was a lot easier to understand how they communicated. The criminal of today tends not to do that, because they have the ability, as we all do, to communicate on the move. Our capability is merely moving with the capability of the criminals we seek to address.

Q169 **Dr Andrew Murrison:** I am not entirely satisfied by that, since you do have an increased range of ways in which you can keep tabs on criminals and investigate them, which draws me to my next point, which is on equipment interference. My first question is: in what proportion of the cases that you deal with is equipment interference used?

Paul Hudson: I do not have the percentage proportion.

Dr Andrew Murrison: What is the ballpark figure?

Paul Hudson: It would be the majority, but it would be difficult to answer in a public forum.

Dr Andrew Murrison: It is a majority of the serious crime.

Paul Hudson: It would be difficult to answer in a public forum.

Dr Andrew Murrison: That is interesting. Okay, perhaps we can come back to that. What concern do you have about the evidential nature of the material that you can generate using equipment interference? In other words, can it be admissible in court, and is it degraded in any way and thus rendered inadmissible?

Paul Hudson: The whole point of law enforcement is to gather evidence that we can place before a court—the best possible evidence. Everything we do is aimed at that. It is covert by nature, but we would not do anything that would degrade that, because when we come to trial we would have to place before the court evidence that we can adduce and provide a fair trial. Nothing we do would reduce the quality of the evidence that we are collecting.

Dr Andrew Murrison: Are you at all concerned that what you do by way of equipment interference poses a risk to wider users? Clearly what you are doing has been characterised as being legalised hacking. I know that is an awful generalisation, a bit like the snooper's charter, and we should really bin those kinds of clichés. Nevertheless, it is the way the *Daily Mail* would present it, for example. That suggests a certain amount of damage that is being done or caused—damage that, since it is associated with the state, is potentially the subject of some sort of comeback against the agencies. Have you any cases where that has happened? I suspect you would not be very happy to share them in a public forum. Are you at all worried that your capability to do this work will at some point come back and bite us?

Paul Hudson: First, I am not. Equipment interference is a covert capability, so nothing that we do under equipment interference would cause any damage or leave any trace, otherwise it would not remain covert for very long. Again, the endgame is to collect evidence to place before a court. If we were causing damage to equipment, that would reduce the ability for the evidence to be alluded to.

Dr Andrew Murrison: You are confident that your activities, by way of equipment interference, will not in particular harm innocent people and render innocent systems compromised or inoperable.

Paul Hudson: Before any deployment, a risk assessment is conducted, and that is part of the authorisation process that would be reviewed by the authorising officer. Subsequently, before authorisation is given, all those risks would be outlined for the judge or the judicial commissioners. Of course that would affect the proportionality and the collateral intrusion that would occur.

Michael Atkinson: I want to cover one thing that Paul said about the majority. We will provide some data, if required, on the use of this type of equipment. We would ask that it is not shared in relation to any reports, because it is very confidential. The other point is that I think it was quite clear, in a couple of the investigations that were shown yesterday, how important this is to us. I will not go into any more details about that.

Matt Long: On the change in crime that we have seen recently, we are starting to see victimless prosecutions, where we have the video of the rape of the child, who is a neonate, too young to talk, but we have the opportunity to use comms data to identify that and to recover that evidence. For CSE, there are very specific examples where the child is unable to report and we use that data to bring a prosecution, which we would not have been able to by any other means. The conviction data, which I am sure can be provided if requested,

shows a year-on-year increase in the responsiveness of the UK to deal earlier with indecent imagery of children across the country. In my particular area, there is a very definitive use that can be seen.

Lord Strasburger: On the evidential quality that comes from computers that have been subject to equipment interference, the other risk is that a guilty person could get off if his defence lawyer discovers that equipment interference has taken place and alleges, for example, that material was planted on the computer at that time. I can see a risk here, and I think others can too, to successful prosecution using evidence from that computer if a third party—in this case you—has had their fingers in it.

Paul Hudson: As we discussed yesterday, equipment interference does not stand alone. As already described, an investigation is a jigsaw puzzle of evidence that is placed before the court, and we would use the current judicial process under the CPIA to ensure that the judge in PII was made fully aware. We would obviously reveal all to the CPS, which would then, through the prosecution counsel, place it before the court and the judge to ensure that the judge knew exactly what had happened, how we did it and our methodology, so that he or she could take a decision on fairness. We would merely place before the court the evidence that is adduced. It would be for the judge to decide.

Q170 Lord Strasburger: Thank you. Can I just talk briefly about intercept as evidence? The lawyers in the Home Office have various views on the admissibility of intercept as evidence. It would be very interesting to hear from policemen at the coalface how helpful or not that would be for you.

Michael Atkinson: We are aware of many studies. It is not our part of the business, although we understand it and know it takes place. It is up to the people who are involved in that area of the business to decide whether they feel it should be used as evidence, and not us.

Q171 Suella Fernandes: Good afternoon. Could you describe for us the oversight and monitoring regime that regulates the process?

Paul Hudson: The majority of the current regime is under the property Act. Originally, the applicant will make an application and lay out their view on proportionality and necessity, as defined, and justification. Under the Bill that is reviewed by a chief officer, who will make a similar assessment. Then it is passed to the judicial commissioner to review and authorise. My understanding is that that is independent, which is welcome. The Act makes it a lot clearer that we have this ability to use it and that we would use it. It is more foreseeable in line with David Anderson's recommendations. Under the Police (Property) Act 1997, the intrusiveness depends on the level of intrusion by the surveillance commissioners. The less intrusive methodologies that we use are authorised and then reviewed, and for the more intrusive methodologies we have to get prior approval under the IP Bill, which is good. We welcome that.

Outside that, my understanding is that the Bill is going to bring together the three different oversight bodies, IOCCO, the OSC and the Security Committee, and make them one. They will continue in that yearly review and that regular inspection of our capability, in line with how it works today. The two different commissioners for the police come to us, look at all

our records, look at how we have deployed, what we have deployed against and have free run of all our databases. It is a much more stringent oversight for us. It is clearer and better in relation to my part of the business.

Suella Fernandes: What practical impact do you think the proposals will have on the process of getting permission to use the powers?

Paul Hudson: Personally, providing there are enough commissioners and the speed is available, there will be no real impact, and the emergency criteria also fit. As I said, it reflects the police Act, so I do not feel that there would be a lot of change.

Michael Atkinson: For CD, we would say that the oversight probably begins at the point when the SPOC becomes involved. Yesterday you heard about the role of the SPOC, and how important it is as a gatekeeper and for the advice it gives.

Suella Fernandes: Sorry to stop you there, but is the SPOC an independent person?

Michael Atkinson: They are independent of the investigation. They have a specific role within the organisation just to apply for communications data. They have first oversight of an application, and then it goes to an independent authorising officer. If it is for subscriber information, it is authorised by an inspector who again is trained and has to go through the full process to understand the application and justify whether it is proportionate and necessary. For anything else, it is a superintendent. Again, he is trained. He understands all the issues involved in making an application.

In addition, clearly we have the IOCCO inspections. These are now undertaken yearly with every force. They interview staff. They obtain some of the applications that we have submitted and review them. They may speak to the investigating officer in order to understand whether the application was submitted correctly. We consider their inspections to be challenging and robust, and we fully support them. They provide us, at times, with advice and guidance in their reports on forces. This can assist with our training. We look at the advice and guidance. We have tradecraft events throughout the year for SPOCs, SPOC managers and DPs, and we ensure that if errors and issues are identified in their reports on policing, we discuss them and look at training to improve what we are doing. We would say that the oversight is good. If the oversight was the same under the new justice commissioner, we would have no issues with that.

Q172 Matt Warman: Just following on from that, what consideration do you give to protecting innocent individuals from the impact when you are investigating people who you obviously have suspicions about? There would be some collateral damage, if you like.

Michael Atkinson: There is clearly an intrusion into somebody's private life whenever we apply for communications data, and throughout the process everybody understands that. We take access to this data very seriously. Again, you heard yesterday about the process and that the initial applicant may be a PC in a station who decides that he is dealing with a theft and the only contact that the victim had was over the phone. They may wish to, and probably will, apply for subscriber details for the person with that phone. That applicant, when he submits that document, will look at necessity and proportionality and whether the application is justified. I cannot sit here and say that they would definitely look at

collateral intrusion, but I would say that when it gets to the SPOC the SPOC will definitely look at collateral intrusion. It is the same for the DP, who will definitely look at collateral intrusion, necessity and proportionality. The gatekeepers of the SPOC will know whether we can even get this data, because it is no good putting in an application if the CSP will not even provide the data, but it happens, probably because people do not understand that some providers will not give us the data.

We have a failure rate and a refusal rate, which shows that we treat this as serious and as an intrusion into people's lives. This varies across forces, but it shows that we can refuse applications because the data is not be there but the SPOC may identify in the very early stages that it is not justified, proportionate and necessary. That can happen at that stage. The next stage is going to the DP. The DP can refuse applications. As a DP I have refused many applications. There are other courses of action that people could take. The role of a DP is not taken lightly. You understand that you are interfering with somebody's private life. I would say that the process that we have deals with those issues.

Matt Warman: Finally, once you have all this data yourselves, once it has been obtained, how do you make sure internally that that data is not vulnerable to being accessed inappropriately, either by your own people or hacked by the outside world?

Michael Atkinson: All SPOCs have PINs so that only they can access the data, which is in stores and in police organisations. Mr Bristow mentioned that no store is definitely safe, but these stores are not the same stores that our other database is on for outside access. People have to have a password to get into it. If we felt that anybody had got into this, we could go back and search who had entered, so I would say that they are very secure.

Suella Fernandes: I have a follow-up question. You talked about the test of necessity and proportionality. What factors are taken into account when you are ascertaining whether this is necessary action and is proportionate?

Michael Atkinson: For a lot of investigations, the first thing I consider is the offence. If I have a murder and I have a victim or a suspect, is it necessary? Of course it is necessary; we need to identify where that person may have been in the last 24 hours or the last two hours. Is it necessary that I need to identify who they had contact with? Yes, of course it is. That is how we conduct the investigation. Alternatively, it could be, as I have had a couple of times, somebody who had given their address over the internet or over the phone. This was several years ago, when fixed-line internet connection records—IPAR—were easier to solve. Somebody would give their address, but the first thing they were applying for was communications data. Was it necessary? You have the suspect's address. Was it proportionate? It was definitely not. Was it justified? No, you have the suspect's address; go and knock on the door. When we make these applications we take into account the offence that we are investigating and the collateral intrusion. Do I need the data for 12 hours when I am looking for my victim in an hour's period? We take all this into consideration, and that is why the process is robust and works well.

Q173 Lord Butler of Brockwell: Some of us were shocked by the use of communications data in the plebgate affair. Do you consider that use of communications data proportionate to the offence that was being examined?

Michael Atkinson: I have not been involved in the plebgate affair. I am not a Metropolitan Police officer. Without my knowing the full knowledge of the offences, what was being investigated, the level of intrusion and what they were applying for, I cannot answer that. I would need to know more information.

The Chairman: Thank you all very much for a very useful, very informative session. Thank you so much for coming along.

National Crime Agency (QQ 26-38)

Evidence heard in public Questions 26-38

Oral Evidence

Taken before the Joint Committee

on Monday 30 November 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Bishop of Chester, Lord Hart of Chilton, and Lord Strasburger.

Witnesses: **Chris Farrimond**, Deputy Director Intelligence Collection, and Keith Bristow, Director General, National Crime Agency, gave evidence.

Q26 **The Chairman:** My apologies for the late running of the earlier session. This was a consequence of Divisions in the House of Lords. You are very welcome. As you know, it is an extremely interesting and important Bill that the Committee is looking at and we very much look forward to the points you have to make to us. Perhaps I could kick off by asking your views on the draft Bill. From your point of view, why have it at all, and how will its proposals affect the work of your own organisations? In that context, which of the powers in the Bill would you regard as new, and which are to be simply consolidated into a new Bill?

Keith Bristow: Thank you Chair. Would you mind if I just made a few opening comments before getting to the specific question? First, thank you very much for seeing us so early. I am representing all senior leaders in law enforcement and policing, because we think this is so important that we need to come before the Committee quickly. Your team has also been very indulgent. I was anxious to bring three senior colleagues who are absolute experts in the breadth of law enforcement.

One of our deputy directors here is Chris Farrimond. He provides many of the law enforcement capabilities to which the draft Bill refers, including lawful interception, CNE and the high-end capabilities provided for the whole of law enforcement. He is a very useful person to have here.

Simon York from HMRC will be able to speak to serious criminality and the taxation system, which again demonstrates the breadth of some of the use that we have to put these capabilities to. Richard Berry is a very experienced police officer in a police force and leads for the National Police Chiefs' Council on communications data. He can speak in some detail about communications data and how it is used across a whole range of policing activities.

Why is this important? Technology has changed the way in which we all lead our lives, which is mostly a good thing for the law-abiding majority. But the reality is that serious and organised criminals in particular, who we target as an agency, also see very significant advantages from technology. That presents us with some very real challenges. The challenges come because the infrastructure of the internet provides some of these people

with significant levels of anonymity, which is a challenge for us. The type of data that is stored and made available to law enforcement does not meet our purposes. The legislation within which we operate is not fit for purpose and was not designed at a time that reflected the age in which we live. The reality is that law enforcement is now experiencing a widening gap. We should remember that law enforcement work is evidential, which is different in many respects from other agencies—the SIA—and it is targeted. The capabilities that we use are brought to protect the public but also to bring people to justice and to discount people and prove alibis.

In the Anderson report, David Anderson identified five purposes that we need for these operational capabilities. Those five purposes remain the same as when we spoke to David Anderson about them. The draft Bill goes a long way towards meeting our operational requirements. We recognise that our requirements are operational and need to be balanced against wider considerations that the Committee, the Government and Parliament in due course will take into account.

Nothing I will say is intended to cut across any of that. We simply want to set out what we need to keep the public safe. One particular concern to which I want to draw your attention—we can put some others in a written submission—relates to internet connection records. The challenge for us is that we believe we need access to all the data that is retained on internet connection records. However, in the draft form of the Bill, that will be limited to three purposes only, which means that data will be retained by communications service providers that we could not request.

As I said, this needs to be balanced against other requirements as well, but it is important to recognise that that limits some of our ability to protect the public and to fight crime.

Lord Butler of Brockwell: Sorry, you said three purposes. What are the three purposes?

Keith Bristow: This is not quite how it is worded in the Bill, but in operational terms one purpose is to resolve IP addresses. It is where a website contains illegal content—or what is called a communications website. For instance, codes of practice may help to refine this and develop our understanding, but it would not include a website where someone could book a rail ticket, which could be hugely important if it related to a missing person. We just need to be clear that data will be retained by service providers to which we cannot request access.

Chairman, you asked specifically about what new powers and new capabilities this Bill would give us. Frankly, it preserves the capabilities that we have always needed, but in a digital age it does not make us more capable of doing things. In operational terms, it brings up to speed what we need to be able to do in a digital age compared to an analogue age. A lot of what we will talk about is comparing what is acceptable to the public, expressed in legislation in the analogue world, how we need to be able to do that in a digital world and how the world has changed.

The Chairman: That is very useful. Thank you very much.

Dr Andrew Murrison: I do not understand this bit about the extra powers that you say you want to have. My understanding is that you could apply for those. Are you specifically talking

about missing persons, because clearly you will be able to get a warrant to get information in relation to serious crime? I am left somewhat confused. Can you clarify it?

Keith Bristow: We cannot request data retained on internet connection records unless it is for the specific purposes that I mentioned. Let me give an example, and Richard is very well qualified to talk about this. If there is a vulnerable missing person—a young person perhaps—and we are concerned about what arrangements they may have put in place to go abroad or to travel, we could not request access to an internet connection record to give us the lead to pursue that point.

Dr Andrew Murrison: Okay, but in relation to a serious crime, as presumably defined by the Serious Crime Act 2007, you would be able to request that data, would you not?

Richard Berry: If I can assist, sir, the major difference with this legislation is that the internet connection records would be retained. If data is retained, for example for business purposes, by a CSP—a communications service provider—then we can apply for that, but forward-facing. The big difference with this Bill is that there will be a retention of those internet connection records and, quite clearly, a process for us to apply for that.

Dr Andrew Murrison: So the information will be retained and you will be able to apply for access to it.

Richard Berry: Yes, but only for the limited categories that Mr Bristow mentioned: so, to resolve an internet protocol address—i.e. to attribute a communication; secondly, to establish whether a person has been using a communications site—Facebook, WhatsApp, those kinds of platforms; and, thirdly, if someone has been accessing illegal content—child abuse imagery or, indeed, terrorist material, that kind of material. There are other policing purposes that we would require access to internet connection records for.

Dr Andrew Murrison: What purposes are those?

Richard Berry: Well, for example; a banking website or, indeed, a travel website. There are case studies that we could furnish the Committee with in writing, if that would be useful, outlining some of those gaps. In a particular case in relation to human trafficking that involves booking flights and the movement of people, we would not be able to obtain that data under the provisions of this Bill. Perhaps I can speak from personal experience having run a large-scale anti-human trafficking operation where 85% of the actionable intelligence came from communications data. That was in the mobile phone era of 2008. We certainly could not repeat that kind of activity now, because the mobile internet communications platforms are where most people now communicate and do those transactions.

Keith Bristow: Might I add two things? Of course the codes of practice, when published, may help us to understand this, but this is our interpretation of the purposes that we can request internet connection records for, and those do not include some of what we will need to access, even though the data is retained.

Dr Andrew Murrison: I am afraid that I am rather confused, because for serious crime—the list is well laid out and, I think, well understood—my understanding is that you would be able to get that information. I am bewildered by what you say. However, there is a question, of

course, about what further cases and crimes you may request information on. I think there would be some resistance to extending the list of serious crimes beyond that given in the 2007 Act, if that is what you are requesting.

Keith Bristow: I am not making any requests; I am setting out the consequence of our understanding, which would allow us to request access to data that has been retained by service providers. You make a point about serious crime, but of course a missing vulnerable person is not a serious crime.

Dr Andrew Murrison: So to cut to the chase, is that your concern?

Keith Bristow: It is one of the concerns, but they are wider than that, because, as we understand it, we can only request data that has been retained by service providers for those three purposes.

The Chairman: So you are telling the Committee that to a certain extent the Bill does not do enough, as far as you are concerned.

Keith Bristow: The question that as law-enforcement professionals we are seeking to answer is: what do we need to protect the public? I am setting out what I believe we need to protect the public, but, as I said in my opening comments, Chair, we absolutely accept that there are wider considerations for this Committee, for Government and for Parliament to consider. I do not think, therefore, that it is for us to set out the operational choices.

The Chairman: You also indicated that any possible codes of conduct that might be constructed might resolve some of these issues.

Keith Bristow: I am not confident that they will resolve them, but they will probably clarify them.

The Chairman: Before Lord Butler asks his question, do any of your colleagues have any comments to make on this?

Richard Berry: Sir, if it would be helpful, the subsection that we are referring to is subsection (4) of Clause 47, which is entitled "Additional restrictions on grant of authorisations".

Lord Butler of Brockwell: I am puzzled, like Dr Murrison. Are we to understand that you could not request communications data to establish locations of suspected persons?

Keith Bristow: If it is for the three purposes that we have set out—

Lord Butler of Brockwell: Which are—

Keith Bristow: If it was a communications website, for instance, if we wanted the internet connection record for a Twitter or Facebook account—an account that is used for communication—we could request the data, and under the Bill the data would be retained and in a format that we could access. We are talking about websites that are not about illegal content, are not communications websites—bearing in mind that these terms are

yet to be defined—and not IP resolution. Those are the areas where we understand that we could request access to the data that the service providers have retained on internet connection records.

Lord Butler of Brockwell: So we are only talking about internet connection records; we are not talking about mobile telephone records.

Keith Bristow: We are talking specifically about ICR.

Lord Butler of Brockwell: This is the distinction: we could still get mobile telephone records to establish the location of a suspect.

Keith Bristow: We could if a mobile phone was used as we currently understand it and as it has been used historically, but of course the really big challenge here is that people are communicating in a different way over the internet. We are confident in our interpretation that we could request access for communication sites, but our understanding is that we could not request the internet connection record of another type of website that might give us an investigative lead, such as one for booking travel tickets or banking.

Lord Butler of Brockwell: It seems to be a very big gap.

Q27 **Victoria Atkins**: Following on from that, would you still be able to contact let us say the travel agency, using your example, to ask whether it had business records to show that this request was made and that X number of tickets were bought?

Keith Bristow: More traditional investigative techniques could be used, but we need the lead in the first place on which travel agent we need to contact. Making the analogue-versus-digital point, the person will not have gone into somewhere on the high street; they will have interacted online. That will be the challenge.

The Chairman: It would be useful when this session is over if you gave us some written evidence with respect to some of the points that you have just made, because, as you can see, members of the Committee are interested in them.

Can I ask a question myself here? It regards current oversight powers. How do the investigatory powers that you currently possess work at the moment? What sort of oversight is there? Will there be a change as a result of this Bill?

Keith Bristow: I will ask Chris to deal with that question, but I will just make a remark to start with. We think that the authorisation and the scrutiny regime is hugely important, because public confidence is what underpins our ability to keep the public safe. It seems to us that because we cannot expose all our operational tradecraft, because we would be exposing it to the very people we want to tackle, we have to have a very clear regime that gives the public confidence that those sensitive techniques are being properly scrutinised. We think this is very important.

Chris Farrimond: There are two aspects to authorisation and oversight, and they are two quite separate parts. The authorisation process for some of our activities is internal, and some of it goes up to the Secretary of State. In each of those cases, whatever the

investigatory power is, we go through a process whereby the applicant has to write down what they require, the proportionality, the necessity, the collateral intrusion, and give their justification. Then, whatever the application is—whether it is a police Act application for intrusive surveillance, a standard surveillance application, or an application for communications data—each application contains the same different aspects of the information: the proportionality, the necessity et cetera. It will then go through the various parts of the chain. It goes to an authorising officer in every case—as I say, in some cases it goes right up to the Secretary of State. Those records are all retained and they are available for inspection at a later date.

We have two oversight regimes at present. One is provided by the Interception of Communications Commissioner's Office—IOCCO—and the other is provided by the Office of Surveillance Commissioners. The oversight regimes that they use are quite similar in that they come in for a pre-arranged inspection, on an annual basis for the most part, and we open up our records to them, give them access to our systems and let them see whatever they wish to see. For a period of a week, they will go through the records and pull out the ones that they want, and we will provide witnesses in the form of investigating officers, the applicants or whoever they wish to speak to. They will write a report based on that. Under the new legislation we envisage something that looks very similar, except that it contains one body rather than two, which we regard as fairly useful.

The Chairman: Thank you very much indeed. Moving to communications data, Miss Atkins.

Q28 **Victoria Atkins:** This is for all witnesses: how do you use communications data and for what purposes?

Richard Berry: If I might share the statistics with the Committee. Very helpfully, they were published on 20 November by the interception commissioner's office based on 100,000 communications data applications, so they are a really good data set. It varies massively. In this example, 80% of communications data applications are for the prevention and detection of crime, and 20% are submitted for interests of national security or, certainly in terms of vulnerable persons, to prevent death or injury in an emergency. So there is an 80:20 split there. From the 80% used for prevention and detection of crime, a quarter of those are in relation to police submissions for burglary, theft and robbery—volume crime.

Just under a quarter are for drug offences and just under 20% are for sexual offences. Then we have smaller and smaller chunks: 12% for harassment, 8% for homicide, fraud and deception, and violence against the person; and 1% for firearms offences. So there is a very broad spectrum of criminality.

Victoria Atkins: How valuable is this data to your investigations? I will come to prosecutions in a moment.

Richard Berry: It is essential, for example for establishing a lead, a seed upon which to build an inquiry. For example, if we take stalking and harassment, which is a very topical issue, around domestic abuse victims. To be able to establish a particular communication and an evidential line of inquiry around a victim being stalked, would be incredibly useful, in fact – vital, to support and corroborate an allegation.

Keith Bristow: We should remember that communications data for us in law enforcement is evidential. Sometimes we do not need to go any further than the communications data. We do not need to turn it into further authorisations for content. It is the "who, what, where, how".[12] Sometimes it is sufficient that we prove that to either eliminate someone from our inquiries, to find a vulnerable person or to start the process of bringing an offender to justice.

Victoria Atkins: I will ask you about context and contact in the context of prosecutions in a moment. How valuable is it in relation to successful prosecutions?

Richard Berry: That can very much depend on the case itself. In a conspiracy case where communication between conspirators is part of proving the offence, it is absolutely vital. In terms of other offences, it could be considered vital. But it could also be important, for example, if we knew a particular person was in a particular place when an offence took place. We might use CCTV evidence to corroborate and identify that person in that location. It really depends on the particular offence being prosecuted and the nature of the evidence we are able to gather.

Q29 Victoria Atkins: Drawing together not just communications data evidence that deals with context but also cell site analysis of where mobile phones are at certain times of the day, is it possible to draw a timeline of a criminal offence in action that you can then present to the jury?

Richard Berry: Absolutely. It is commonplace now to produce a sequence of events—that is the term we use—and an analytical chart on the sequence of events showing communications and where people work geolocated by their phones, and to supplement that with other forms of evidence.

Q30 Victoria Atkins: Mr Lincoln mentioned very briefly an example of a warrant not being extended in circumstances where, for example, the target perhaps has got hold of another telephone. How common is that sort of activity in organised crime gangs?

Richard Berry: Operational security is as important to criminality as it is to law enforcement.

People regularly are changing their devices, setting up false accounts and swapping devices. All those tactics and techniques are used. It takes a lot of investigation to be able to understand who is using a device at a particular time, what it is being used for at that time and how it fits into the overall picture of that criminality.

Victoria Atkins: Just to get the point into context, the length of call can in itself help prosecution counsel when suggesting to a jury, for example, that that is the moment at which the drugs were dropped.

Richard Berry: Absolutely.

[12] Witness correction: clarification that what should have been said is "It is the who, when, where, how." What, refers to lawful intercept which is not incorporated in the meaning of communications data.

Chris Farrimond: I offer one or two other examples. One is about the range of use of comms data. The National Crime Agency receives the bulk of referrals in respect of child sexual exploitation on behalf of the United Kingdom. Just from one source, we receive about 1,500 per month. In many cases, resolving that IP address is the only way we can identify the victim or the perpetrator. I am sad to say that in 14% of cases we cannot resolve it at all. There is no way to do it and there is no way of identifying that victim or perpetrator. That is single-source intelligence and, if we did not act on that, there is no other way of doing it. We have similar examples, as will Richard, with missing children where there is no other way of identifying them but for this methodology.

Simon York: Can I give you an HMRC perspective on this? Last year, we made just over 10,000 communications data requests. That supported 560 investigations. I think that those numbers represent the complexity and the conspiracy involved in many of these cases. Almost 100% of our requests were in relation to preventing and detecting crime in contrast to the wider needs of the NCA.

This can be in relation to anything from smuggling to tax fraud to trying to criminally exploit HMRC's repayment systems. Literally billions of pounds are at stake here. Last year, investigations where we used communications data and intercept together prevented around £2 billion loss to the UK Exchequer. That is how important it is to us.

Victoria Atkins: Is it fair to say that a lot of those investigations involve serious organised crime gangs?

Simon York: Almost all of them, yes.

Q31 Lord Butler of Brockwell: Leading on from that, was I right to understand that you were saying that internet connection records although useful are not, as defined in the Bill, sufficient to help you to identify all senders, the users of all IP addresses?

Chris Farrimond: Some IP addresses are more difficult to resolve than others. A standard home broadband is a static IP and it is relatively easy to resolve down to an address. When you use your mobile phone, your IP address is allocated to that phone just for the few seconds that you make that search and then it is allocated to someone else somewhere else in the country. It is really complicated.

The IP addresses get swapped around mobile phones, tablets and everything else around the country a lot of times per day. Trying to get complete resolution for some of the more complex ones is not possible at the moment. We believe that ICRs will allow us to close that gap quite considerably.

Lord Butler of Brockwell: Right, but it will not close it completely. I understand that you cannot always resolve IP addresses, but if you get internet connection records you can identify the users of the address.

Chris Farrimond: I am afraid that my knowledge of technology is not good enough to give 100% on this, but we believe that it will massively close the gap. It could be up to the whole amount.

Lord Butler of Brockwell: Just going back to the three purposes for which you can use it, you say that you can attribute connection from an IPR. Then you could discover that someone had been a user of Facebook. How does it help in a criminal investigation to discover that they are a user of Facebook?

Chris Farrimond: It means that we can ask Facebook. Certainly, when we are talking about vulnerable children, threats to life or anything like that, we find that communication sites of that type are extremely helpful.

Lord Butler of Brockwell: If you go to Facebook, are you going to the content and not just the communications data? Would you seek a warrant? If you did seek a warrant, would that be effective with Facebook?

Chris Farrimond: At that stage we would not need to go for an interception warrant, because we would not be intercepting communications in the course of their transmission.

Lord Butler of Brockwell: I understand.

Chris Farrimond: It would be stored data at that stage, so we would be looking for the stored data that Facebook had in that instance.

Lord Butler of Brockwell: And Facebook would be able to tell you with whom the person who was suspected had been communicating with.

Chris Farrimond: It should be able to do that, yes.

Lord Butler of Brockwell: I understand. Thank you.

Q32 Stuart C McDonald: What would you say is the operational case for 12 months in particular being the maximum time for requiring the detention of communications data and internet connection records?

Chris Farrimond: I know that the Home Office, who were here before, gave you some figures. We have a table here that it might be helpful for us to include in our written submission to you, but let me give you some examples. In a 2012 survey right across policing in the UK, of all crime types within 0 to six months approximately 84% of comms data was applicable: that is to say, when we needed it, 84% fell within the 0 to six months, 13% within the seven to 12 months, and 3% in the 12 months-plus. But that does not give the whole picture. For child abuse, only 42% fell within the 0 to six months, and 52% fell within the seven to 12 months. There are also figures for terrorism offences, sexual offences and financial offences. We can give those figures, but this quite clearly shows that the closer you are to the date, generally speaking as soon as the investigators get hold of the case they are going to want to get the data, but sometimes it takes a bit longer, for whatever reason. For instance, we do not immediately get the referrals that I spoke about a few minutes ago involving child sexual exploitation; sometimes it can take a few months for them to come through, which may be the reason for the 52%. Either way, I think it shows pretty consistently that 12 months is a reasonable point at which to draw the line.

Keith Bristow: It is worth differentiating between types of investigation. As an agency and collectively, we sometimes investigate criminals; we are proactive, so we want to know how they were transacting at that moment. With reactive investigations, of course, often we do not know what data we need until an offence has been reported to us and we are some way down the track with an investigation. I suspect that is exactly why, with child abuse, data retention is further down the line in time terms.

Simon York: The position for HMRC is a little different. Our figures show that more than 50% falls into the six to 12 month period. Indeed, quite a lot falls beyond 12 months. We are doing a lot of reactive, or historical, analysis. We have some real-time stuff, perhaps smuggling, but if it is more in the tax evasion area it can be a lot more historical; if it involves the use tax returns, we will not even do that analysis until 12 months after the year ends. We are in quite a different position from that of the National Crime Agency. Overall, we feel that 12 months is a reasonable balance to be struck, but we have a lot of cases that fall within that six to 12 month period.

Stuart C McDonald: Okay. We will obviously need to look in detail at the tables that you provide, but is there not a danger that what you are describing there is practice rather than what is essential. Is there analysis that shows that the information that you get from records that are between six and months old ends up being crucial to a case?

Richard Berry: If I may help with that, there are types of crime that require communications data perhaps two or three years after the offence has been committed and subsequently reported. Boiler-room fraud is a classic example of the picture of the criminality only emerges some years later, so clearly the 12-month period for the retention of communications data is not particularly useful for that particular criminality. Also, criminal justice processes kick in. If we are looking at an alibi or identifying further witnesses, subsequent applications for communications data up to that 12-month period can also be incredibly useful for a particular investigation because of the interests of justice and if the disclosure regime highlights that further inquiries are required by the police at that time. We have not mapped it, but I understand that that kind of data may be produced in the future and we can start to understand the value of data at a particular point in time for a particular crime type.

Q33 **Stuart C McDonald:** Thank you very much. Finally, as far as you are aware, how do such rights of access up to 12 months compare to rights of access that colleagues in other jurisdictions have?

Richard Berry: Our comparison is with the Australians, who have recently been given a two-year retention period. I understand that in the original period the data retention directive was for 24 months, so we are striking a balance in many respects. Twelve months seems to be the period when the optimal value is obtained by law enforcement.

Stuart C McDonald: In terms of internet connection records, this is fairly unique, is it not?

Richard Berry: We do not have that evidence.

Q34 **Bishop of Chester**: This is the first time I have spoken on this matter and I need to declare that I have no interests. Can I go to the question of the length of the period? Is there

frustration that it is only 12 months in serious cases in HMRC, for example, where you cannot go back beyond 12 months? Australia has fixed two years. Is this a source of frustration to you in your investigation of crime?

Keith Bristow: I think there is a need to understand the mindset of the investigator. All the best investigators are rigorously focused on doing what they need to do to keep the public safe. Chris has given numbers demonstrating 0 to six months and six to 12 months. There are also numbers that show data after 12 months that would have benefited the investigation. My sense is that there is some science that points to 12 months, but there is also the professional judgment that, when you look at the numbers, the data appears to be less relevant after 12 months. Of course our mindset that is we want every opportunity to protect the public in every set of circumstances, but that has to be balanced against other considerations.

Bishop of Chester: Are you sometimes slowed up by having to analyse seized equipment—laptops or whatever—which, as I understand it, is often in a queue, takes time and extends investigations?

Keith Bristow: Operation Notarise was an operation, led by the NCA and involving every police force in the UK, against people who were exploiting children online. We ended up seizing tens of thousands of devices that were relevant, which could be a digital camera, an iPhone: all the devices that we all understand. When you have that volume of devices, triaging those involves a lot of professional judgment about which are the most important to collect the most evidence from of the high end of high risk. We do not always get that right, because, frankly, there is not the capability, even with the private sector, to everything at pace all the time.

Bishop of Chester: Does the 12-month retention period hang over that investigation?

Keith Bristow: No, because once we have seized a media device, we have seized it. We then get to the point where we analyse its content. The 12 months is more about the data that is retained by service providers to enable us to access the data. It is not about the hard content of the device.

Bishop of Chester: So the analysis of the various devices that you have just described does not throw up the need to—

Chris Farrimond: It can do, because stored messages on a computer can point to an IP address, and, yes, we have had examples, even recently when they were one day over the date.

Keith Bristow: With victim ID, for instance, if we get an image and we want to identify the victim—a child who has been exploited—and we want to rescue that child, the reality is that we might need the communications data that sits around some of those communications to try to resolve the identity of the victim.

Q35 **Lord Strasburger:** The Counter-Terrorism and Security Bill earlier this year created the power to resolve IP addresses. How many times have you used that, and how does it differ from the power in this Bill?

Chris Farrimond: The provisions in that Act are not all in force yet. Although we use exactly the same communications service providers as our counterterrorist colleagues—so we use exactly the same access—we still cannot resolve the technology and the systems in place where the communications service provider has not yet caught up completely with the provisions of that Act. Therefore we cannot fully resolve all IP addresses, which brings me to the 14%.

Q36 **Lord Hart of Chilton**: Fifty-five years ago at university, I joined Amnesty International and I think that technically I might still be a member. That is my declaration of interest. What safeguards do you have in place to prevent unauthorised access to the communications data and other materials you hold? I imagine that the criminal mind is always at work trying to break in.

Chris Farrimond: The vast majority of communications data is held by the communications service providers. We can only access it in the certain circumstances that I have outlined around necessity, proportionality etcetera, in which case in the NCA's case, it comes into the NCA and is held on the same systems as all the other evidence we have.

It is treated in exactly the same way, to the same specification and safeguards, as all our criminal intelligence data, which is held to a high level. Although there have been various attempts to get on our website, they have only ever managed to get on the outward-facing one. They have never managed to get anywhere near the inward-facing one. That is not a challenge. We are satisfied with the security of our system.

Lord Hart of Chilton: Just to be clear, how many break-ins have there been?

Chris Farrimond: I believe there have been one or two to our outward-facing website.

Lord Hart of Chilton: And how did they come about?

Chris Farrimond: I am afraid that, again, my technical knowledge defeats me.

Keith Bristow: As regards most of the attacks that we get on our outward-facing website, the catalyst is that we have taken on some cybercriminals. The community that supports people like that do a DDoS attack on our website to try to get us to take it down. We spend considerable resource and energy making sure we keep that site secure. That is not the system where we retain our intelligence and our evidence. It is the front face and it appeals to the public that we tell them what we are doing and are as transparent as we can be. We rarely take it down, but sometimes as the result of a DDoS attack we have had to do so to protect it.

Lord Hart of Chilton: How much has that cost you?

Keith Bristow: I would need to come back to you with a number, but it is significant.

Simon York: Similarly from an HMRC perspective, we hold this information on secure systems in secure buildings and we have specially selected and trained staff who are the only people with access to this type of material.

Lord Hart of Chilton: And you have not had any breaches?

Simon York: No.

Richard Berry: The single point of contact in David Anderson's report. they have pin numbers and they are all vetted to a high standard and they work in secure environments. There are a range of security measures, as well as the physical security, to ensure that there are no breaches of unlawful access of that information.

Lord Hart of Chilton: So, as far as you are concerned, there have been no breaches?

Richard Berry: Absolutely.

Lord Butler of Brockwell: The Inland Revenue had a notorious example of where they lost CDs in the post. Are you absolutely sure you have systems that prevent anything like that happening with this sort of data?

Simon York: Absolutely. After that event, which was quite some years ago now, there was a very comprehensive review of all our security processes. Interestingly, the data that was allegedly on those discs has never surfaced in any way to be used in criminality or otherwise in the UK.

Lord Hart of Chilton: Did you ever recover it?

Simon York: No.

Keith Bristow: From an NCA perspective, we invest huge amounts of energy and time in data security. What I could not do is give you a 100% cast-iron guarantee that there will never be a breach. When you mix well-intentioned people into any of these systems, it needs only one failing for data to get into the public domain. But within what is physically and legally possible, we treat this information security as our top risk.

Q37 **Matt Warman**: Can you talk me through what value equipment interference provides your organisation and what justification there is for you to be able to conduct equipment interference?

Chris Farrimond: We use property interference at the moment, which is authorised under the Police Act. We use it for a range of purposes, ranging from pretty much every-day relatively routine activities right up to far more high end. The difficulty is that trying to describe any of those techniques in this setting probably would be inappropriate, but I would certainly be very happy to explain them in a great deal more detail if we had the opportunity to do so.

Matt Warman: More generally, in that case, how often do anticipate being required to use equipment interference in the future?

Chris Farrimond: That is quite difficult to answer, because I could not have predicted the IP revolution that there has been or the digital change that we have seen. The change from traditional telephony into IP-based communications has been enormous and the pace has been really difficult to keep up with. I could not make any prediction about just how much we would use this. I suspect that our limitation would be around our own resources and

our own capability rather than the demand. The demand for quite a lot of the services that I am allowed to manage within the NCA outstrips supply.

Keith Bristow: To give you a trend, I think it is fair to say that as law-abiding citizens it is no different—more of what we do now is online using digital devices. I imagine that the trend will peak, but I think that we will be doing more rather than less that reflects the behaviour of the criminals who we are targeting.

Richard Berry: To give a police perspective on this, we use equipment interference regularly, really for tracing vulnerable and suicidal missing persons.

The other point I would like to make is that there has to be some consideration from our perspective of the integrity of the information contained on a device that is interfered with. For example, to comply with the requirements of Section 69 of the Police and Criminal Evidence Act on the integrity of computer information, there might be considerations perhaps prohibiting the creation of data purporting to be communications data on that particular device or perhaps removing such data from that device. The evidential integrity of that device might be particularly important. Perhaps we can expand on that in a written submission.

Q38 **Matt Warman:** Finally, on demand versus supply, do your organisations currently have the capabilities technically and in terms of manpower to do what is needed? Do you anticipate seriously being able to ramp that up?

Chris Farrimond: We have the capability, and I anticipate that, if required, we could ramp it up, yes.

Keith Bristow: The change for the NCA and the transformation programme that it is going to go through—the Government announced the funding for that last year—mostly relates to our digital capabilities. As criminals go online, we need to be as adept in the digital environment as we are in the physical environment. Those capabilities are going to be invested in on behalf of the whole law enforcement community and not just us, because we provide those to our colleagues in HMRC, for instance.

Richard Berry: RUSI recommendation 5 as being that law enforcement should have a comprehensive digital investigations intelligence programme. A number of colleagues are here and we are part of that programme. Building capabilities is certainly one of those priorities.

The Chairman: Thank you very much indeed. Again, apologies for the delay because of the votes. This has been a fascinating session and we look forward to receiving your written evidence to supplement what you have told us today.

Keith Bristow: Chairman, do you mind if I just reiterate Chris's offer? We want to be open and transparent with the Committee and the public viewing this or reading the report are hugely important. However, we cannot betray all our tradecraft to criminals.

The Chairman: Of course not.

Keith Bristow: There is an open offer to the Committee, and I know that I speak for my colleagues as well; if you want to look at what we do, whether in a comms data unit or about equipment interference, we will brief you at a higher level of classification to help with your deliberations. Thank you for your time.

The Chairman: That is very generous of you. Thank you very much indeed.

Temporary Detective Superintendent Matt Long, Child Exploitation and Online Protection Command at the National Crime Agency (QQ 162-173)

Evidence heard in public Questions 162-173

Oral Evidence

Taken before the Joint Committee

on Wednesday 16 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Lord Butler of Brockwell, Bishop of Chester, Lord Strasburger.

Witness: **Temporary Detective Superintendent Matt Long**, Child Exploitation and Online Protection Command at the National Crime Agency, gave evidence.

Q162 The Chairman: A very warm welcome to all of you. I was just saying that this is a rather large room—a bit like Mussolini's waiting room, if you ever saw that. You are miles away down there. Can I say how valuable the Committee thought our visit was yesterday, by the way, as an introduction? It was extremely useful and gave us a lot of food for thought. I am going to start the first question and my colleagues will come in afterwards. Do feel free, each of you, to comment on the answers, if you so wish.

This question is very general. What is your view on the Bill? To what extent do you think it is necessary, and how will it improve and affect the operational work of your respective organisations? Do you feel it goes far enough?

Michael Atkinson: Thank you, Lord Chairman, for inviting us here today. We are pleased that yesterday was of benefit, hopefully to you all, to see how our working practices take place.

Could I first introduce us? My name is Michael Atkinson. I am the secretary for the National Police Council's Data Communications Group, and I work for ACC Richard Berry, who appeared in front of you several weeks ago. To my right is Detective Superintendent Matthew Long. Matthew is a deputy head of UK operations within CEOP, which is part of the NCA. I hope that Matthew and I may be able to provide you with some evidence on our use of CD and how this relates to the Bill. On my left is Detective Superintendent Paul Hudson. Paul leads and is the head of the Metropolitan Police Service's technical surveillance unit. He will, I hope, deal with any questions you have in relation to equipment interference.

The Chairman: Thank you very much indeed. Of course, we met some of you yesterday. Anyway, what is your view of the Bill? Is it right? Is it necessary? Does it do what you want it to do, and does it go far enough for you?

Michael Atkinson: I suppose it is no good me sitting here talking to you about the change in technology. You have probably all seen enough, since you have been in this Committee, about how technology has changed. What is happening with policing? We are struggling. How are we struggling? We are struggling to keep pace with how victims, witnesses and criminals use technology. In many investigations, we try to use CD as evidence. It is causing us problems to obtain this evidence. We use CD in many investigations: theft, child sexual exploitation, homicides or frauds—a wide spectrum of offences. Our inability to obtain this data is increasing, for various reasons. Some CSPs do not retain the data for long enough in certain services. Some CSPs are outside our jurisdiction; we have difficulty with their laws in obtaining the data, and some CSPs outside our jurisdiction will not assist us. Also, some of the data is not retained. I have said that it is not retained for long enough, but the actual data that we require is not retained. We believe that this Bill will assist in closing some, but not all, of the gap that we are currently experiencing.

Paul Hudson: Lord Chairman, if I may I will also bring you the EI perspective on this. We would seek further capability. The Bill currently provides extra oversight, which we welcome, but it is all about serious crime. On very rare occasions, as I hope we demonstrated yesterday, we might use EI to protect the most vulnerable people, and that might not be in serious crime; it might be to save them from doing harm to themselves. So, in the emergency provision, we would look for something that legitimises that use of EI: to protect the most vulnerable people from harm.

Q163 **Mr Hanson:** Thanks for coming in. My apologies for yesterday; I was on another Select Committee elsewhere in the building. For my benefit, but also to put it on the record, it would be really useful if you could give a couple of concrete examples of how the current use of powers has led to convictions or, as you have said, has been of help in providing safety or rescue to individuals.

Michael Atkinson: Unfortunately, you were not there yesterday, because you would have been provided with evidence that clearly showed how we use communications data in protecting the vulnerable. You would have seen and had explained various examples of young missing children and people who were going to commit suicide. Unfortunately, we did not manage to save everybody.

We use the vast majority of communications data to protect the vulnerable and save people's lives. In addition to that, our use is predominantly in two areas of our business: proactive and reactive investigations. That is what we use communications data for. In proactive investigations, we may use it to identify a conspiracy and people talking to each other. We may use it to identify people's whereabouts at certain times. We also use it to identify other leads; for example, somebody may have phoned a travel agent and it gives us a lead so that we can go there. We may be able to get that information, take further steps and make further inquiries. So in proactive investigations, we use it in various ways.

In reactive investigations, the offence has predominantly taken place. Murder is probably one of the more serious crimes that we look at. My background is as an SIO, and in every murder investigation in which I have been involved we have used communications data. Why do we use it? We need to identify where the victim was and where their last movements were. It may be over a 24-hour period or it may be just a relevant period of time. We also look at and identify people with whom they have had contact and, again,

that may be over a 24-hour period or a specific time period. That is no different when we identify a suspect: we would look at their data, their locations and who they are talking to. We use it across various offences.

We use data together with forensics and other data opportunities, such as ANPR and CCTV. In 2012, we undertook some work and identified communications data use in 95% of all serious crime prosecutions. We use communications data in 100% of counterterrorist investigations. Matt will probably give you some more examples of how it is used in CEOP and its work.

Matt Long: In answer to your question, the Bill is essential and invaluable. I will give you two operational examples. First, the National Crime Agency's CEOP receives between 1,300 and 1,500 referrals every month from the National Center for Missing & Exploited Children in the US, the majority of which are reported online. Every one of those is a child at risk or a suspect for us to identify, and with the majority the starting point is the communications data. For each of those, myriad further victims or suspects may be identified who we need to follow, so in the daily, weekly and monthly movement in the National Crime Agency that is the volume that we need communication data to support.

A more personal example is that I am still the senior investigating officer for Operation Notarise. Within that operation, we arrested 745 offenders nationally. Every single one of those offenders who we arrested had a comms data application attached to them, and some had multiple applications. Within that investigation, we safeguarded over 518 children, so as the senior investigating officer I see it as a tool in the toolbox, although not the only tool; it is complemented by other tools such as open source. To summarise, there is that daily, weekly protection of children. In the large-scale and small-scale operations, we need it critically to progress.

Mr Hanson: What areas of new media are you not able to access now because of the way in which the legislation is currently framed?

Matt Long: A very simple example, which I was going to come on to later but will bring in now, because it illustrates it, is in grooming. With the grooming of a child on a communications platform that is online only, if we request that data we want to know who that child is talking to. Who is that offender? Are they talking to other offenders or children? There is some data that we simply cannot get. If that is the only route by which they are communicating, which is increasingly the case, it simply is not available to us.

Mr Hanson: What is the difference between seizing PCs and seizing mobile telephones to get that data, as opposed to having the powers under this Bill?

Matt Long: You need to have the computer or the phone to be able to do it in the first place. Our difficulty is that we may have a report that has come across from the National Center for Missing & Exploited Children, which says that a child is in communication with an individual, and we do not know where they are and do not have the devices. It is quite easy once you have the offender in custody and you can go to the device. Then we will proportionally assess those devices and see how many offenders we can identify and other routes that we can follow. Ultimately, sometimes the very first step is that communications data. Without it, we cannot take the first step, which is the identification.

Q164 Lord Strasburger: Good afternoon, gentlemen. Is accessing internet connection records, if that can be done, essential for the purposes of IP address resolution and identifying persons of interest?

Michael Atkinson: I have spent several hours in one of the UK CSPs for mobile phones. I cannot sit here and say that I am a technical person who understands the technical issues to do with how telephones are used, how they retain the data, what data they retain and what they might need to do to provide ICRs. What I can say is that they are assuring me that, without the retention of ICRs, they will not be able to solve internet protocol resolutions. They also tell me that we will not get the evidence that we need in order to undertake further investigations of people who may be of interest to us. Matt has given you one example. Another example is a terrorist investigation. We do not do live inception in all terrorist investigations that we undertake. We may do investigations for months and months, identifying intelligence, connections between people and what the suspects are intending to do. If we are investigating some suspects and have some intelligence but it is insufficient to arrest, we would like to know whether they have gone to a website on how to make a bomb, whether they have gone to a website of a major shopping place in the UK, whether they have gone to a website where they might wish to book some tickets to leave the country. Currently, we cannot get that. We believe, and we are told by the communication service providers, that ICR will solve this.

Q165 Shabana Mahmood: Last week we had oral evidence from a number of smaller CSPs, and one of the things they said on internet connection records that struck me as important was that the internet connection record would probably provide a useless bit of information. If you had a mobile telephone for a young missing child, for example, all the ICR could tell you is that that phone had been connected to Twitter or Facebook for 24 hours a day for the last six months from the point at which the phone was bought, because many of the apps that are used are automatically connected to the internet. I have just checked my phone. I have background app refresh on, which means that it is automatically connected on a 24-hour basis. Is there a danger that lots of information that you collect from internet connection records is just useless: it gives you no additional investigative assistance?

Michael Atkinson: Again, we look at what we are being told by the largest CSPs. If we have a missing person, we conduct a lot of inquiries. CD may not be our first inquiry. We have other inquiries to undertake, but we may identify that the missing person has a phone. What better way to trace them than through the cell site to identify where they are?

Sometimes phones have been turned off, but we can get back the fact that they have been talking on Twitter to somebody. Even just by getting that back, we can go to Twitter. Twitter, and not necessarily just that company but other companies, will help us to identify vulnerable missing people. They will identify to us that they may have been in contact with certain people, who would give us further lines of inquiry and may allow us to identify where this missing person is. ICR could tell us that they have booked a train ticket. They have gone to a train line; it looks as though they have booked a train ticket. We can make inquiries with them. We can see that they have. Maybe we can locate where they have gone. The CSPs that I have spoken to have made it clear that ICRs would assist us.

Shabana Mahmood: National Rail Enquiries, which is the main app that most people use for booking their train ticket, is on 24-hour background app refresh. I suppose this Bill is

introducing a whole new regime for internet connection records. My question is: is it necessary? Will it just give you oodles and oodles of useless information? If you are trying to trace a child, you know they are on Twitter and you can get into their Twitter account or ask their friends, who are more likely to be able to tell you what the Twitter or Facebook activity of that young person was.

Michael Atkinson: That is what we try to do, but there is always this issue. Matthew explained the relationship with grooming. We can get a lot of information that can assist us to identify where they are. We realise that there is collateral intrusion. We realise that there are risks to this, but on the other hand there are children and missing people. Are we willing to go further to try to save a life or to bring the person back to their family?

Stuart C McDonald: First of all, just following up on those points, in quite a lot of missing persons cases, for example, it must be pretty straightforward to establish whether the missing person has a Twitter or Facebook account and then, once you have done that, you can go to these communications service providers and find information about who they have been contacting and so on.

Michael Atkinson: Sometimes we can, yes.

Stuart C McDonald: How often are you frustrated in trying to find what people have been doing to communicate with others?

Michael Atkinson: I cannot sit here and say how often it happens. What I can say is that it does happen. Some companies will not assist us; some companies that are outside our jurisdiction will not support us and help us with identification, but many of them do.

Q166 Stuart C McDonald: Now, as you will understand, the proposal is for communication service providers to be required to retain communications data and internet connection records for 12 months. What is your comment on 12 months being the specific limit? Would you want more than that, or could you cope with six months or three months?

Michael Atkinson: It is interesting that this has come up several times. I was involved in the 2012 Bill. In 2012, we undertook a survey across policing. Sixty-four law enforcement organisations, in 2012, undertook applications for communications data. We received replies from 63 organisations. They undertook a two-week survey in every SPOC unit. The unit that you went into yesterday recorded, over a two-week period, every application that went through the unit in each of the 63 organisations. That gave us a really good breakdown of how we use communications data, but also of the history of the data that we are applying for. To give you an example, we covered nearly 10,000 pieces of data and applications. That is what this survey was about. Nine per cent of those applications were for sexual offences. What was interesting was that 37% of that 9% of data that we applied for was more than six months old. We would say, and you can see, that retaining the data for more than six months is very important. We also identified that 1% of all the data was for terrorist investigations, and 27% of that data was more than six months old. Now, I know we are writing to you, Lord Chairman, and we would be happy to provide that data to you with our submission, but it provided us with some really good background and understanding of why. Further, it shows what is more than nine months old or 12 months old, so there is more data there.

What is really interesting is a document produced by IOCCO on 20 November, only last month, which is a breakdown of communications data and applications. It shows over 100,000 communications data applications, 19% of which were in relation to sexual offences. Two things jumped straight out at me. First, this is a 100% increase from the survey that we did in 2012. Secondly, 37% of roughly 19,000 is over 7,000. We would say that, if we retain data for only six months, hundreds if not thousands of suspects for sexual offences would likely evade prosecution.

Stuart C McDonald: Can I just pick you up on that, though? That information is very useful, but it does not tell us how crucial that information is at six months old, 12 months old or whatever it is. I suspect it is almost impossible to gather that, but what is your personal view?

Michael Atkinson: We have had the conversation about when we undertake investigations. A homicide investigation is a bit like a jigsaw, but you need all the pieces to make the picture. I will have communications data. I may have CCTV. I may have forensic data. I may have ANPR. There are quite a few pieces to make up that jigsaw. What you cannot necessarily say is which piece was crucial in detecting and prosecuting that person for that offence. The whole picture helps to prosecute, not an individual piece.

Q167 Victoria Atkins: Following on from that, perhaps this is an easier way of looking at it. Is there a single serious organisation case that you have investigated and taken to trial in the last decade that has not involved mobile phone records or records of telephone communications?

Michael Atkinson: I cannot sit here, hand on heart, and say 100% that there is, but the data shows that in 2012 we used it for 95% of all serious and organised crimes. I would be very surprised if any serious and organised crime case went to court where we had not used communications data.

Matt Long: Perhaps I could elaborate further for you. I gave the example earlier of Operation Notarise, with 745 arrests and 518 children safeguarded. In that operation, within a 12-month period, we resolved 92% of data. If I had 12 months, I would get a 92% return. If that dropped to six months, I would lose six out of 10 of the pieces of data. Out of six months, we would lose 60% of that offending population. If you dropped it by a further 12 weeks, I would have lost 87% of the lines of inquiry presented to me. In that case, the first point was communication data. To answer your question about what the impact would have been on me in that operation, it would have been those percentages at those time stamps. When you think about that in relation to that operation, the majority of the offenders in that operation were not known to law enforcement. It is not as though I have another database that I can check and then identify that person by some other means. I simply cannot do that. When you think that 15% of those people were in a position of trust—they were a teacher, a scoutmaster or in another position where they were the guardians of our children—it is very unlikely that I will find another route, because those individuals have gone through criminal record checks. They have gone through the very good safeguards that we have as a country, but effectively they have beaten them. That example shows you what the output and the outcome would be if you reduced the length of retention in those ways.

Michael Atkinson: Sorry, Lord Chairman, could I just cover one other point? We do not use communications data just to prosecute people. We clearly use it also to prove that people have not committed an offence. The defence uses communications data. For our more serious cases, especially if we are talking about counterterrorism, homicides and serious and organised crime, can take six months, nine months or over a year to come to trial. If the defence serves their defence statement on us six or seven months after the offence has taken place and we only retain data for six months, it would prevent them from having a fair trial and it would prevent us from checking alibis and defence statements, so we believe that 12 months is the appropriate period.

Matt Long: Can I make one final point on that? The other thing, going back to your point, is that victims do not disclose on day one when the communications data is available to us. It may take them weeks or months to gain the confidence to disclose. Then, we do not get a consequential order of victims so that we know that A leads to B who leads to C. It might be that A leads to E, E leads to another 100, and we have to review them. All that takes time. It is not necessarily even at that first instance of the offence when we need the data. We need to conduct the investigation and be allowed sufficient time to do that. Sometimes that can take months.

Q168 **Dr Andrew Murrison:** Good afternoon, gentlemen. Twenty years ago, we did not have any of this technology available to us, so setting aside crimes that are specific to modern communications such as online paedophilia et cetera, it follows from what you have said that since you now do have access to all these investigative modalities, your clear-up rate should have been dramatically improved and your ability to secure missing people, for example, should have been improved. Is that in fact the case?

Paul Hudson: As much as we have greater technological investigative powers, the criminals we seek to arrest and bring before the courts also have greater technological ability to avoid us. We have seen that the increase in technology, the mobile nature of communication and the mobile nature of making meetings have made it more difficult. The criminal of 20 years ago used to meet at a safe house and it was a lot easier to understand how they communicated. The criminal of today tends not to do that, because they have the ability, as we all do, to communicate on the move. Our capability is merely moving with the capability of the criminals we seek to address.

Q169 **Dr Andrew Murrison:** I am not entirely satisfied by that, since you do have an increased range of ways in which you can keep tabs on criminals and investigate them, which draws me to my next point, which is on equipment interference. My first question is: in what proportion of the cases that you deal with is equipment interference used?

Paul Hudson: I do not have the percentage proportion.

Dr Andrew Murrison: What is the ballpark figure?

Paul Hudson: It would be the majority, but it would be difficult to answer in a public forum.

Dr Andrew Murrison: It is a majority of the serious crime.

Paul Hudson: It would be difficult to answer in a public forum.

Dr Andrew Murrison: That is interesting. Okay, perhaps we can come back to that. What concern do you have about the evidential nature of the material that you can generate using equipment interference? In other words, can it be admissible in court, and is it degraded in any way and thus rendered inadmissible?

Paul Hudson: The whole point of law enforcement is to gather evidence that we can place before a court—the best possible evidence. Everything we do is aimed at that. It is covert by nature, but we would not do anything that would degrade that, because when we come to trial we would have to place before the court evidence that we can adduce and provide a fair trial. Nothing we do would reduce the quality of the evidence that we are collecting.

Dr Andrew Murrison: Are you at all concerned that what you do by way of equipment interference poses a risk to wider users? Clearly what you are doing has been characterised as being legalised hacking. I know that is an awful generalisation, a bit like the snooper's charter, and we should really bin those kinds of clichés. Nevertheless, it is the way the *Daily Mail* would present it, for example. That suggests a certain amount of damage that is being done or caused—damage that, since it is associated with the state, is potentially the subject of some sort of comeback against the agencies. Have you any cases where that has happened? I suspect you would not be very happy to share them in a public forum. Are you at all worried that your capability to do this work will at some point come back and bite us?

Paul Hudson: First, I am not. Equipment interference is a covert capability, so nothing that we do under equipment interference would cause any damage or leave any trace, otherwise it would not remain covert for very long. Again, the endgame is to collect evidence to place before a court. If we were causing damage to equipment, that would reduce the ability for the evidence to be alluded to.

Dr Andrew Murrison: You are confident that your activities, by way of equipment interference, will not in particular harm innocent people and render innocent systems compromised or inoperable.

Paul Hudson: Before any deployment, a risk assessment is conducted, and that is part of the authorisation process that would be reviewed by the authorising officer. Subsequently, before authorisation is given, all those risks would be outlined for the judge or the judicial commissioners. Of course that would affect the proportionality and the collateral intrusion that would occur.

Michael Atkinson: I want to cover one thing that Paul said about the majority. We will provide some data, if required, on the use of this type of equipment. We would ask that it is not shared in relation to any reports, because it is very confidential. The other point is that I think it was quite clear, in a couple of the investigations that were shown yesterday, how important this is to us. I will not go into any more details about that.

Matt Long: On the change in crime that we have seen recently, we are starting to see victimless prosecutions, where we have the video of the rape of the child, who is a neonate, too young to talk, but we have the opportunity to use comms data to identify that and to recover that evidence. For CSE, there are very specific examples where the child is unable to report and we use that data to bring a prosecution, which we would not have been able to by any other means. The conviction data, which I am sure can be provided if requested,

shows a year-on-year increase in the responsiveness of the UK to deal earlier with indecent imagery of children across the country. In my particular area, there is a very definitive use that can be seen.

Lord Strasburger: On the evidential quality that comes from computers that have been subject to equipment interference, the other risk is that a guilty person could get off if his defence lawyer discovers that equipment interference has taken place and alleges, for example, that material was planted on the computer at that time. I can see a risk here, and I think others can too, to successful prosecution using evidence from that computer if a third party—in this case you—has had their fingers in it.

Paul Hudson: As we discussed yesterday, equipment interference does not stand alone. As already described, an investigation is a jigsaw puzzle of evidence that is placed before the court, and we would use the current judicial process under the CPIA to ensure that the judge in PII was made fully aware. We would obviously reveal all to the CPS, which would then, through the prosecution counsel, place it before the court and the judge to ensure that the judge knew exactly what had happened, how we did it and our methodology, so that he or she could take a decision on fairness. We would merely place before the court the evidence that is adduced. It would be for the judge to decide.

Q170 Lord Strasburger: Thank you. Can I just talk briefly about intercept as evidence? The lawyers in the Home Office have various views on the admissibility of intercept as evidence. It would be very interesting to hear from policemen at the coalface how helpful or not that would be for you.

Michael Atkinson: We are aware of many studies. It is not our part of the business, although we understand it and know it takes place. It is up to the people who are involved in that area of the business to decide whether they feel it should be used as evidence, and not us.

Q171 Suella Fernandes: Good afternoon. Could you describe for us the oversight and monitoring regime that regulates the process?

Paul Hudson: The majority of the current regime is under the property Act. Originally, the applicant will make an application and lay out their view on proportionality and necessity, as defined, and justification. Under the Bill that is reviewed by a chief officer, who will make a similar assessment. Then it is passed to the judicial commissioner to review and authorise. My understanding is that that is independent, which is welcome. The Act makes it a lot clearer that we have this ability to use it and that we would use it. It is more foreseeable in line with David Anderson's recommendations. Under the Police (Property) Act 1997, the intrusiveness depends on the level of intrusion by the surveillance commissioners. The less intrusive methodologies that we use are authorised and then reviewed, and for the more intrusive methodologies we have to get prior approval under the IP Bill, which is good. We welcome that.

Outside that, my understanding is that the Bill is going to bring together the three different oversight bodies, IOCCO, the OSC and the Security Committee, and make them one. They will continue in that yearly review and that regular inspection of our capability, in line with how it works today. The two different commissioners for the police come to us, look at all

our records, look at how we have deployed, what we have deployed against and have free run of all our databases. It is a much more stringent oversight for us. It is clearer and better in relation to my part of the business.

Suella Fernandes: What practical impact do you think the proposals will have on the process of getting permission to use the powers?

Paul Hudson: Personally, providing there are enough commissioners and the speed is available, there will be no real impact, and the emergency criteria also fit. As I said, it reflects the police Act, so I do not feel that there would be a lot of change.

Michael Atkinson: For CD, we would say that the oversight probably begins at the point when the SPOC becomes involved. Yesterday you heard about the role of the SPOC, and how important it is as a gatekeeper and for the advice it gives.

Suella Fernandes: Sorry to stop you there, but is the SPOC an independent person?

Michael Atkinson: They are independent of the investigation. They have a specific role within the organisation just to apply for communications data. They have first oversight of an application, and then it goes to an independent authorising officer. If it is for subscriber information, it is authorised by an inspector who again is trained and has to go through the full process to understand the application and justify whether it is proportionate and necessary. For anything else, it is a superintendent. Again, he is trained. He understands all the issues involved in making an application.

In addition, clearly we have the IOCCO inspections. These are now undertaken yearly with every force. They interview staff. They obtain some of the applications that we have submitted and review them. They may speak to the investigating officer in order to understand whether the application was submitted correctly. We consider their inspections to be challenging and robust, and we fully support them. They provide us, at times, with advice and guidance in their reports on forces. This can assist with our training. We look at the advice and guidance. We have tradecraft events throughout the year for SPOCs, SPOC managers and DPs, and we ensure that if errors and issues are identified in their reports on policing, we discuss them and look at training to improve what we are doing. We would say that the oversight is good. If the oversight was the same under the new justice commissioner, we would have no issues with that.

Q172 Matt Warman: Just following on from that, what consideration do you give to protecting innocent individuals from the impact when you are investigating people who you obviously have suspicions about? There would be some collateral damage, if you like.

Michael Atkinson: There is clearly an intrusion into somebody's private life whenever we apply for communications data, and throughout the process everybody understands that. We take access to this data very seriously. Again, you heard yesterday about the process and that the initial applicant may be a PC in a station who decides that he is dealing with a theft and the only contact that the victim had was over the phone. They may wish to, and probably will, apply for subscriber details for the person with that phone. That applicant, when he submits that document, will look at necessity and proportionality and whether the application is justified. I cannot sit here and say that they would definitely look at

collateral intrusion, but I would say that when it gets to the SPOC the SPOC will definitely look at collateral intrusion. It is the same for the DP, who will definitely look at collateral intrusion, necessity and proportionality. The gatekeepers of the SPOC will know whether we can even get this data, because it is no good putting in an application if the CSP will not even provide the data, but it happens, probably because people do not understand that some providers will not give us the data.

We have a failure rate and a refusal rate, which shows that we treat this as serious and as an intrusion into people's lives. This varies across forces, but it shows that we can refuse applications because the data is not be there but the SPOC may identify in the very early stages that it is not justified, proportionate and necessary. That can happen at that stage. The next stage is going to the DP. The DP can refuse applications. As a DP I have refused many applications. There are other courses of action that people could take. The role of a DP is not taken lightly. You understand that you are interfering with somebody's private life. I would say that the process that we have deals with those issues.

Matt Warman: Finally, once you have all this data yourselves, once it has been obtained, how do you make sure internally that that data is not vulnerable to being accessed inappropriately, either by your own people or hacked by the outside world?

Michael Atkinson: All SPOCs have PINs so that only they can access the data, which is in stores and in police organisations. Mr Bristow mentioned that no store is definitely safe, but these stores are not the same stores that our other database is on for outside access. People have to have a password to get into it. If we felt that anybody had got into this, we could go back and search who had entered, so I would say that they are very secure.

Suella Fernandes: I have a follow-up question. You talked about the test of necessity and proportionality. What factors are taken into account when you are ascertaining whether this is necessary action and is proportionate?

Michael Atkinson: For a lot of investigations, the first thing I consider is the offence. If I have a murder and I have a victim or a suspect, is it necessary? Of course it is necessary; we need to identify where that person may have been in the last 24 hours or the last two hours. Is it necessary that I need to identify who they had contact with? Yes, of course it is. That is how we conduct the investigation. Alternatively, it could be, as I have had a couple of times, somebody who had given their address over the internet or over the phone. This was several years ago, when fixed-line internet connection records—IPAR—were easier to solve. Somebody would give their address, but the first thing they were applying for was communications data. Was it necessary? You have the suspect's address. Was it proportionate? It was definitely not. Was it justified? No, you have the suspect's address; go and knock on the door. When we make these applications we take into account the offence that we are investigating and the collateral intrusion. Do I need the data for 12 hours when I am looking for my victim in an hour's period? We take all this into consideration, and that is why the process is robust and works well.

Q173 Lord Butler of Brockwell: Some of us were shocked by the use of communications data in the plebgate affair. Do you consider that use of communications data proportionate to the offence that was being examined?

Michael Atkinson: I have not been involved in the plebgate affair. I am not a Metropolitan Police officer. Without my knowing the full knowledge of the offences, what was being investigated, the level of intrusion and what they were applying for, I cannot answer that. I would need to know more information.

The Chairman: Thank you all very much for a very useful, very informative session. Thank you so much for coming along.

National Police Chiefs' Council (QQ 26-38)

Evidence heard in public Questions 26-38

Oral Evidence

Taken before the Joint Committee

on Monday 30 November 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Bishop of Chester, Lord Hart of Chilton, and Lord Strasburger.

Witness: **Richard Berry**, Assistant Chief Constable, National Police Chiefs' Council, gave evidence.

Q26 **The Chairman:** My apologies for the late running of the earlier session. This was a consequence of Divisions in the House of Lords. You are very welcome. As you know, it is an extremely interesting and important Bill that the Committee is looking at and we very much look forward to the points you have to make to us. Perhaps I could kick off by asking your views on the draft Bill. From your point of view, why have it at all, and how will its proposals affect the work of your own organisations? In that context, which of the powers in the Bill would you regard as new, and which are to be simply consolidated into a new Bill?

Keith Bristow: Thank you Chair. Would you mind if I just made a few opening comments before getting to the specific question? First, thank you very much for seeing us so early. I am representing all senior leaders in law enforcement and policing, because we think this is so important that we need to come before the Committee quickly. Your team has also been very indulgent. I was anxious to bring three senior colleagues who are absolute experts in the breadth of law enforcement.

One of our deputy directors here is Chris Farrimond. He provides many of the law enforcement capabilities to which the draft Bill refers, including lawful interception, CNE and the high-end capabilities provided for the whole of law enforcement. He is a very useful person to have here.

Simon York from HMRC will be able to speak to serious criminality and the taxation system, which again demonstrates the breadth of some of the use that we have to put these capabilities to. Richard Berry is a very experienced police officer in a police force and leads for the National Police Chiefs' Council on communications data. He can speak in some detail about communications data and how it is used across a whole range of policing activities.

Why is this important? Technology has changed the way in which we all lead our lives, which is mostly a good thing for the law-abiding majority. But the reality is that serious and organised criminals in particular, who we target as an agency, also see very significant advantages from technology. That presents us with some very real challenges. The challenges come because the infrastructure of the internet provides some of these people

with significant levels of anonymity, which is a challenge for us. The type of data that is stored and made available to law enforcement does not meet our purposes. The legislation within which we operate is not fit for purpose and was not designed at a time that reflected the age in which we live. The reality is that law enforcement is now experiencing a widening gap. We should remember that law enforcement work is evidential, which is different in many respects from other agencies—the SIA—and it is targeted. The capabilities that we use are brought to protect the public but also to bring people to justice and to discount people and prove alibis.

In the Anderson report, David Anderson identified five purposes that we need for these operational capabilities. Those five purposes remain the same as when we spoke to David Anderson about them. The draft Bill goes a long way towards meeting our operational requirements. We recognise that our requirements are operational and need to be balanced against wider considerations that the Committee, the Government and Parliament in due course will take into account.

Nothing I will say is intended to cut across any of that. We simply want to set out what we need to keep the public safe. One particular concern to which I want to draw your attention—we can put some others in a written submission—relates to internet connection records. The challenge for us is that we believe we need access to all the data that is retained on internet connection records. However, in the draft form of the Bill, that will be limited to three purposes only, which means that data will be retained by communications service providers that we could not request.

As I said, this needs to be balanced against other requirements as well, but it is important to recognise that that limits some of our ability to protect the public and to fight crime.

Lord Butler of Brockwell: Sorry, you said three purposes. What are the three purposes?

Keith Bristow: This is not quite how it is worded in the Bill, but in operational terms one purpose is to resolve IP addresses. It is where a website contains illegal content—or what is called a communications website. For instance, codes of practice may help to refine this and develop our understanding, but it would not include a website where someone could book a rail ticket, which could be hugely important if it related to a missing person. We just need to be clear that data will be retained by service providers to which we cannot request access.

Chairman, you asked specifically about what new powers and new capabilities this Bill would give us. Frankly, it preserves the capabilities that we have always needed, but in a digital age it does not make us more capable of doing things. In operational terms, it brings up to speed what we need to be able to do in a digital age compared to an analogue age. A lot of what we will talk about is comparing what is acceptable to the public, expressed in legislation in the analogue world, how we need to be able to do that in a digital world and how the world has changed.

The Chairman: That is very useful. Thank you very much.

Dr Andrew Murrison: I do not understand this bit about the extra powers that you say you want to have. My understanding is that you could apply for those. Are you specifically talking

about missing persons, because clearly you will be able to get a warrant to get information in relation to serious crime? I am left somewhat confused. Can you clarify it?

Keith Bristow: We cannot request data retained on internet connection records unless it is for the specific purposes that I mentioned. Let me give an example, and Richard is very well qualified to talk about this. If there is a vulnerable missing person—a young person perhaps—and we are concerned about what arrangements they may have put in place to go abroad or to travel, we could not request access to an internet connection record to give us the lead to pursue that point.

Dr Andrew Murrison: Okay, but in relation to a serious crime, as presumably defined by the Serious Crime Act 2007, you would be able to request that data, would you not?

Richard Berry: If I can assist, sir, the major difference with this legislation is that the internet connection records would be retained. If data is retained, for example for business purposes, by a CSP—a communications service provider—then we can apply for that, but forward-facing. The big difference with this Bill is that there will be a retention of those internet connection records and, quite clearly, a process for us to apply for that.

Dr Andrew Murrison: So the information will be retained and you will be able to apply for access to it.

Richard Berry: Yes, but only for the limited categories that Mr Bristow mentioned: so, to resolve an internet protocol address—i.e. to attribute a communication; secondly, to establish whether a person has been using a communications site—Facebook, WhatsApp, those kinds of platforms; and, thirdly, if someone has been accessing illegal content—child abuse imagery or, indeed, terrorist material, that kind of material. There are other policing purposes that we would require access to internet connection records for.

Dr Andrew Murrison: What purposes are those?

Richard Berry: Well, for example; a banking website or, indeed, a travel website. There are case studies that we could furnish the Committee with in writing, if that would be useful, outlining some of those gaps. In a particular case in relation to human trafficking that involves booking flights and the movement of people, we would not be able to obtain that data under the provisions of this Bill. Perhaps I can speak from personal experience having run a large-scale anti-human trafficking operation where 85% of the actionable intelligence came from communications data. That was in the mobile phone era of 2008. We certainly could not repeat that kind of activity now, because the mobile internet communications platforms are where most people now communicate and do those transactions.

Keith Bristow: Might I add two things? Of course the codes of practice, when published, may help us to understand this, but this is our interpretation of the purposes that we can request internet connection records for, and those do not include some of what we will need to access, even though the data is retained.

Dr Andrew Murrison: I am afraid that I am rather confused, because for serious crime—the list is well laid out and, I think, well understood—my understanding is that you would be able to get that information. I am bewildered by what you say. However, there is a question, of

course, about what further cases and crimes you may request information on. I think there would be some resistance to extending the list of serious crimes beyond that given in the 2007 Act, if that is what you are requesting.

Keith Bristow: I am not making any requests; I am setting out the consequence of our understanding, which would allow us to request access to data that has been retained by service providers. You make a point about serious crime, but of course a missing vulnerable person is not a serious crime.

Dr Andrew Murrison: So to cut to the chase, is that your concern?

Keith Bristow: It is one of the concerns, but they are wider than that, because, as we understand it, we can only request data that has been retained by service providers for those three purposes.

The Chairman: So you are telling the Committee that to a certain extent the Bill does not do enough, as far as you are concerned.

Keith Bristow: The question that as law-enforcement professionals we are seeking to answer is: what do we need to protect the public? I am setting out what I believe we need to protect the public, but, as I said in my opening comments, Chair, we absolutely accept that there are wider considerations for this Committee, for Government and for Parliament to consider. I do not think, therefore, that it is for us to set out the operational choices.

The Chairman: You also indicated that any possible codes of conduct that might be constructed might resolve some of these issues.

Keith Bristow: I am not confident that they will resolve them, but they will probably clarify them.

The Chairman: Before Lord Butler asks his question, do any of your colleagues have any comments to make on this?

Richard Berry: Sir, if it would be helpful, the subsection that we are referring to is subsection (4) of Clause 47, which is entitled "Additional restrictions on grant of authorisations".

Lord Butler of Brockwell: I am puzzled, like Dr Murrison. Are we to understand that you could not request communications data to establish locations of suspected persons?

Keith Bristow: If it is for the three purposes that we have set out—

Lord Butler of Brockwell: Which are—

Keith Bristow: If it was a communications website, for instance, if we wanted the internet connection record for a Twitter or Facebook account—an account that is used for communication—we could request the data, and under the Bill the data would be retained and in a format that we could access. We are talking about websites that are not about illegal content, are not communications websites—bearing in mind that these terms are

yet to be defined—and not IP resolution. Those are the areas where we understand that we could request access to the data that the service providers have retained on internet connection records.

Lord Butler of Brockwell: So we are only talking about internet connection records; we are not talking about mobile telephone records.

Keith Bristow: We are talking specifically about ICR.

Lord Butler of Brockwell: This is the distinction: we could still get mobile telephone records to establish the location of a suspect.

Keith Bristow: We could if a mobile phone was used as we currently understand it and as it has been used historically, but of course the really big challenge here is that people are communicating in a different way over the internet. We are confident in our interpretation that we could request access for communication sites, but our understanding is that we could not request the internet connection record of another type of website that might give us an investigative lead, such as one for booking travel tickets or banking.

Lord Butler of Brockwell: It seems to be a very big gap.

Q27 **Victoria Atkins**: Following on from that, would you still be able to contact let us say the travel agency, using your example, to ask whether it had business records to show that this request was made and that X number of tickets were bought?

Keith Bristow: More traditional investigative techniques could be used, but we need the lead in the first place on which travel agent we need to contact. Making the analogue-versus-digital point, the person will not have gone into somewhere on the high street; they will have interacted online. That will be the challenge.

The Chairman: It would be useful when this session is over if you gave us some written evidence with respect to some of the points that you have just made, because, as you can see, members of the Committee are interested in them.

Can I ask a question myself here? It regards current oversight powers. How do the investigatory powers that you currently possess work at the moment? What sort of oversight is there? Will there be a change as a result of this Bill?

Keith Bristow: I will ask Chris to deal with that question, but I will just make a remark to start with. We think that the authorisation and the scrutiny regime is hugely important, because public confidence is what underpins our ability to keep the public safe. It seems to us that because we cannot expose all our operational tradecraft, because we would be exposing it to the very people we want to tackle, we have to have a very clear regime that gives the public confidence that those sensitive techniques are being properly scrutinised. We think this is very important.

Chris Farrimond: There are two aspects to authorisation and oversight, and they are two quite separate parts. The authorisation process for some of our activities is internal, and some of it goes up to the Secretary of State. In each of those cases, whatever the

investigatory power is, we go through a process whereby the applicant has to write down what they require, the proportionality, the necessity, the collateral intrusion, and give their justification. Then, whatever the application is—whether it is a police Act application for intrusive surveillance, a standard surveillance application, or an application for communications data—each application contains the same different aspects of the information: the proportionality, the necessity et cetera. It will then go through the various parts of the chain. It goes to an authorising officer in every case—as I say, in some cases it goes right up to the Secretary of State. Those records are all retained and they are available for inspection at a later date.

We have two oversight regimes at present. One is provided by the Interception of Communications Commissioner's Office—IOCCO—and the other is provided by the Office of Surveillance Commissioners. The oversight regimes that they use are quite similar in that they come in for a pre-arranged inspection, on an annual basis for the most part, and we open up our records to them, give them access to our systems and let them see whatever they wish to see. For a period of a week, they will go through the records and pull out the ones that they want, and we will provide witnesses in the form of investigating officers, the applicants or whoever they wish to speak to. They will write a report based on that. Under the new legislation we envisage something that looks very similar, except that it contains one body rather than two, which we regard as fairly useful.

The Chairman: Thank you very much indeed. Moving to communications data, Miss Atkins.

Q28 **Victoria Atkins:** This is for all witnesses: how do you use communications data and for what purposes?

Richard Berry: If I might share the statistics with the Committee. Very helpfully, they were published on 20 November by the interception commissioner's office based on 100,000 communications data applications, so they are a really good data set. It varies massively. In this example, 80% of communications data applications are for the prevention and detection of crime, and 20% are submitted for interests of national security or, certainly in terms of vulnerable persons, to prevent death or injury in an emergency. So there is an 80:20 split there. From the 80% used for prevention and detection of crime, a quarter of those are in relation to police submissions for burglary, theft and robbery—volume crime.

Just under a quarter are for drug offences and just under 20% are for sexual offences. Then we have smaller and smaller chunks: 12% for harassment, 8% for homicide, fraud and deception, and violence against the person; and 1% for firearms offences. So there is a very broad spectrum of criminality.

Victoria Atkins: How valuable is this data to your investigations? I will come to prosecutions in a moment.

Richard Berry: It is essential, for example for establishing a lead, a seed upon which to build an inquiry. For example, if we take stalking and harassment, which is a very topical issue, around domestic abuse victims. To be able to establish a particular communication and an evidential line of inquiry around a victim being stalked, would be incredibly useful, in fact – vital, to support and corroborate an allegation.

Keith Bristow: We should remember that communications data for us in law enforcement is evidential. Sometimes we do not need to go any further than the communications data. We do not need to turn it into further authorisations for content. It is the "who, what, where, how".[13] Sometimes it is sufficient that we prove that to either eliminate someone from our inquiries, to find a vulnerable person or to start the process of bringing an offender to justice.

Victoria Atkins: I will ask you about context and contact in the context of prosecutions in a moment. How valuable is it in relation to successful prosecutions?

Richard Berry: That can very much depend on the case itself. In a conspiracy case where communication between conspirators is part of proving the offence, it is absolutely vital. In terms of other offences, it could be considered vital. But it could also be important, for example, if we knew a particular person was in a particular place when an offence took place. We might use CCTV evidence to corroborate and identify that person in that location. It really depends on the particular offence being prosecuted and the nature of the evidence we are able to gather.

Q29 **Victoria Atkins:** Drawing together not just communications data evidence that deals with context but also cell site analysis of where mobile phones are at certain times of the day, is it possible to draw a timeline of a criminal offence in action that you can then present to the jury?

Richard Berry: Absolutely. It is commonplace now to produce a sequence of events—that is the term we use—and an analytical chart on the sequence of events showing communications and where people work geolocated by their phones, and to supplement that with other forms of evidence.

Q30 **Victoria Atkins:** Mr Lincoln mentioned very briefly an example of a warrant not being extended in circumstances where, for example, the target perhaps has got hold of another telephone. How common is that sort of activity in organised crime gangs?

Richard Berry: Operational security is as important to criminality as it is to law enforcement.

People regularly are changing their devices, setting up false accounts and swapping devices. All those tactics and techniques are used. It takes a lot of investigation to be able to understand who is using a device at a particular time, what it is being used for at that time and how it fits into the overall picture of that criminality.

Victoria Atkins: Just to get the point into context, the length of call can in itself help prosecution counsel when suggesting to a jury, for example, that that is the moment at which the drugs were dropped.

Richard Berry: Absolutely.

[13] Witness correction: clarification that what should have been said is "It is the who, when, where, how." What, refers to lawful intercept which is not incorporated in the meaning of communications data.

Chris Farrimond: I offer one or two other examples. One is about the range of use of comms data. The National Crime Agency receives the bulk of referrals in respect of child sexual exploitation on behalf of the United Kingdom. Just from one source, we receive about 1,500 per month. In many cases, resolving that IP address is the only way we can identify the victim or the perpetrator. I am sad to say that in 14% of cases we cannot resolve it at all. There is no way to do it and there is no way of identifying that victim or perpetrator. That is single-source intelligence and, if we did not act on that, there is no other way of doing it. We have similar examples, as will Richard, with missing children where there is no other way of identifying them but for this methodology.

Simon York: Can I give you an HMRC perspective on this? Last year, we made just over 10,000 communications data requests. That supported 560 investigations. I think that those numbers represent the complexity and the conspiracy involved in many of these cases. Almost 100% of our requests were in relation to preventing and detecting crime in contrast to the wider needs of the NCA.

This can be in relation to anything from smuggling to tax fraud to trying to criminally exploit HMRC's repayment systems. Literally billions of pounds are at stake here. Last year, investigations where we used communications data and intercept together prevented around £2 billion loss to the UK Exchequer. That is how important it is to us.

Victoria Atkins: Is it fair to say that a lot of those investigations involve serious organised crime gangs?

Simon York: Almost all of them, yes.

Q31 Lord Butler of Brockwell: Leading on from that, was I right to understand that you were saying that internet connection records although useful are not, as defined in the Bill, sufficient to help you to identify all senders, the users of all IP addresses?

Chris Farrimond: Some IP addresses are more difficult to resolve than others. A standard home broadband is a static IP and it is relatively easy to resolve down to an address. When you use your mobile phone, your IP address is allocated to that phone just for the few seconds that you make that search and then it is allocated to someone else somewhere else in the country. It is really complicated.

The IP addresses get swapped around mobile phones, tablets and everything else around the country a lot of times per day. Trying to get complete resolution for some of the more complex ones is not possible at the moment. We believe that ICRs will allow us to close that gap quite considerably.

Lord Butler of Brockwell: Right, but it will not close it completely. I understand that you cannot always resolve IP addresses, but if you get internet connection records you can identify the users of the address.

Chris Farrimond: I am afraid that my knowledge of technology is not good enough to give 100% on this, but we believe that it will massively close the gap. It could be up to the whole amount.

Lord Butler of Brockwell: Just going back to the three purposes for which you can use it, you say that you can attribute connection from an IPR. Then you could discover that someone had been a user of Facebook. How does it help in a criminal investigation to discover that they are a user of Facebook?

Chris Farrimond: It means that we can ask Facebook. Certainly, when we are talking about vulnerable children, threats to life or anything like that, we find that communication sites of that type are extremely helpful.

Lord Butler of Brockwell: If you go to Facebook, are you going to the content and not just the communications data? Would you seek a warrant? If you did seek a warrant, would that be effective with Facebook?

Chris Farrimond: At that stage we would not need to go for an interception warrant, because we would not be intercepting communications in the course of their transmission.

Lord Butler of Brockwell: I understand.

Chris Farrimond: It would be stored data at that stage, so we would be looking for the stored data that Facebook had in that instance.

Lord Butler of Brockwell: And Facebook would be able to tell you with whom the person who was suspected had been communicating with.

Chris Farrimond: It should be able to do that, yes.

Lord Butler of Brockwell: I understand. Thank you.

Q32 Stuart C McDonald: What would you say is the operational case for 12 months in particular being the maximum time for requiring the detention of communications data and internet connection records?

Chris Farrimond: I know that the Home Office, who were here before, gave you some figures. We have a table here that it might be helpful for us to include in our written submission to you, but let me give you some examples. In a 2012 survey right across policing in the UK, of all crime types within 0 to six months approximately 84% of comms data was applicable: that is to say, when we needed it, 84% fell within the 0 to six months, 13% within the seven to 12 months, and 3% in the 12 months-plus. But that does not give the whole picture. For child abuse, only 42% fell within the 0 to six months, and 52% fell within the seven to 12 months. There are also figures for terrorism offences, sexual offences and financial offences. We can give those figures, but this quite clearly shows that the closer you are to the date, generally speaking as soon as the investigators get hold of the case they are going to want to get the data, but sometimes it takes a bit longer, for whatever reason. For instance, we do not immediately get the referrals that I spoke about a few minutes ago involving child sexual exploitation; sometimes it can take a few months for them to come through, which may be the reason for the 52%. Either way, I think it shows pretty consistently that 12 months is a reasonable point at which to draw the line.

Keith Bristow: It is worth differentiating between types of investigation. As an agency and collectively, we sometimes investigate criminals; we are proactive, so we want to know how they were transacting at that moment. With reactive investigations, of course, often we do not know what data we need until an offence has been reported to us and we are some way down the track with an investigation. I suspect that is exactly why, with child abuse, data retention is further down the line in time terms.

Simon York: The position for HMRC is a little different. Our figures show that more than 50% falls into the six to 12 month period. Indeed, quite a lot falls beyond 12 months. We are doing a lot of reactive, or historical, analysis. We have some real-time stuff, perhaps smuggling, but if it is more in the tax evasion area it can be a lot more historical; if it involves the use tax returns, we will not even do that analysis until 12 months after the year ends. We are in quite a different position from that of the National Crime Agency. Overall, we feel that 12 months is a reasonable balance to be struck, but we have a lot of cases that fall within that six to 12 month period.

Stuart C McDonald: Okay. We will obviously need to look in detail at the tables that you provide, but is there not a danger that what you are describing there is practice rather than what is essential. Is there analysis that shows that the information that you get from records that are between six and months old ends up being crucial to a case?

Richard Berry: If I may help with that, there are types of crime that require communications data perhaps two or three years after the offence has been committed and subsequently reported. Boiler-room fraud is a classic example of the picture of the criminality only emerges some years later, so clearly the 12-month period for the retention of communications data is not particularly useful for that particular criminality. Also, criminal justice processes kick in. If we are looking at an alibi or identifying further witnesses, subsequent applications for communications data up to that 12-month period can also be incredibly useful for a particular investigation because of the interests of justice and if the disclosure regime highlights that further inquiries are required by the police at that time. We have not mapped it, but I understand that that kind of data may be produced in the future and we can start to understand the value of data at a particular point in time for a particular crime type.

Q33 **Stuart C McDonald:** Thank you very much. Finally, as far as you are aware, how do such rights of access up to 12 months compare to rights of access that colleagues in other jurisdictions have?

Richard Berry: Our comparison is with the Australians, who have recently been given a two-year retention period. I understand that in the original period the data retention directive was for 24 months, so we are striking a balance in many respects. Twelve months seems to be the period when the optimal value is obtained by law enforcement.

Stuart C McDonald: In terms of internet connection records, this is fairly unique, is it not?

Richard Berry: We do not have that evidence.

Q34 **Bishop of Chester**: This is the first time I have spoken on this matter and I need to declare that I have no interests. Can I go to the question of the length of the period? Is there

frustration that it is only 12 months in serious cases in HMRC, for example, where you cannot go back beyond 12 months? Australia has fixed two years. Is this a source of frustration to you in your investigation of crime?

Keith Bristow: I think there is a need to understand the mindset of the investigator. All the best investigators are rigorously focused on doing what they need to do to keep the public safe. Chris has given numbers demonstrating 0 to six months and six to 12 months. There are also numbers that show data after 12 months that would have benefited the investigation. My sense is that there is some science that points to 12 months, but there is also the professional judgment that, when you look at the numbers, the data appears to be less relevant after 12 months. Of course our mindset that is we want every opportunity to protect the public in every set of circumstances, but that has to be balanced against other considerations.

Bishop of Chester: Are you sometimes slowed up by having to analyse seized equipment—laptops or whatever—which, as I understand it, is often in a queue, takes time and extends investigations?

Keith Bristow: Operation Notarise was an operation, led by the NCA and involving every police force in the UK, against people who were exploiting children online. We ended up seizing tens of thousands of devices that were relevant, which could be a digital camera, an iPhone: all the devices that we all understand. When you have that volume of devices, triaging those involves a lot of professional judgment about which are the most important to collect the most evidence from of the high end of high risk. We do not always get that right, because, frankly, there is not the capability, even with the private sector, to everything at pace all the time.

Bishop of Chester: Does the 12-month retention period hang over that investigation?

Keith Bristow: No, because once we have seized a media device, we have seized it. We then get to the point where we analyse its content. The 12 months is more about the data that is retained by service providers to enable us to access the data. It is not about the hard content of the device.

Bishop of Chester: So the analysis of the various devices that you have just described does not throw up the need to—

Chris Farrimond: It can do, because stored messages on a computer can point to an IP address, and, yes, we have had examples, even recently when they were one day over the date.

Keith Bristow: With victim ID, for instance, if we get an image and we want to identify the victim—a child who has been exploited—and we want to rescue that child, the reality is that we might need the communications data that sits around some of those communications to try to resolve the identity of the victim.

Q35 **Lord Strasburger:** The Counter-Terrorism and Security Bill earlier this year created the power to resolve IP addresses. How many times have you used that, and how does it differ from the power in this Bill?

Chris Farrimond: The provisions in that Act are not all in force yet. Although we use exactly the same communications service providers as our counterterrorist colleagues—so we use exactly the same access—we still cannot resolve the technology and the systems in place where the communications service provider has not yet caught up completely with the provisions of that Act. Therefore we cannot fully resolve all IP addresses, which brings me to the 14%.

Q36 **Lord Hart of Chilton**: Fifty-five years ago at university, I joined Amnesty International and I think that technically I might still be a member. That is my declaration of interest. What safeguards do you have in place to prevent unauthorised access to the communications data and other materials you hold? I imagine that the criminal mind is always at work trying to break in.

Chris Farrimond: The vast majority of communications data is held by the communications service providers. We can only access it in the certain circumstances that I have outlined around necessity, proportionality etcetera, in which case in the NCA's case, it comes into the NCA and is held on the same systems as all the other evidence we have.

It is treated in exactly the same way, to the same specification and safeguards, as all our criminal intelligence data, which is held to a high level. Although there have been various attempts to get on our website, they have only ever managed to get on the outward-facing one. They have never managed to get anywhere near the inward-facing one. That is not a challenge. We are satisfied with the security of our system.

Lord Hart of Chilton: Just to be clear, how many break-ins have there been?

Chris Farrimond: I believe there have been one or two to our outward-facing website.

Lord Hart of Chilton: And how did they come about?

Chris Farrimond: I am afraid that, again, my technical knowledge defeats me.

Keith Bristow: As regards most of the attacks that we get on our outward-facing website, the catalyst is that we have taken on some cybercriminals. The community that supports people like that do a DDoS attack on our website to try to get us to take it down. We spend considerable resource and energy making sure we keep that site secure. That is not the system where we retain our intelligence and our evidence. It is the front face and it appeals to the public that we tell them what we are doing and are as transparent as we can be. We rarely take it down, but sometimes as the result of a DDoS attack we have had to do so to protect it.

Lord Hart of Chilton: How much has that cost you?

Keith Bristow: I would need to come back to you with a number, but it is significant.

Simon York: Similarly from an HMRC perspective, we hold this information on secure systems in secure buildings and we have specially selected and trained staff who are the only people with access to this type of material.

Lord Hart of Chilton: And you have not had any breaches?

Simon York: No.

Richard Berry: The single point of contact in David Anderson's report. they have pin numbers and they are all vetted to a high standard and they work in secure environments. There are a range of security measures, as well as the physical security, to ensure that there are no breaches of unlawful access of that information.

Lord Hart of Chilton: So, as far as you are concerned, there have been no breaches?

Richard Berry: Absolutely.

Lord Butler of Brockwell: The Inland Revenue had a notorious example of where they lost CDs in the post. Are you absolutely sure you have systems that prevent anything like that happening with this sort of data?

Simon York: Absolutely. After that event, which was quite some years ago now, there was a very comprehensive review of all our security processes. Interestingly, the data that was allegedly on those discs has never surfaced in any way to be used in criminality or otherwise in the UK.

Lord Hart of Chilton: Did you ever recover it?

Simon York: No.

Keith Bristow: From an NCA perspective, we invest huge amounts of energy and time in data security. What I could not do is give you a 100% cast-iron guarantee that there will never be a breach. When you mix well-intentioned people into any of these systems, it needs only one failing for data to get into the public domain. But within what is physically and legally possible, we treat this information security as our top risk.

Q37 **Matt Warman**: Can you talk me through what value equipment interference provides your organisation and what justification there is for you to be able to conduct equipment interference?

Chris Farrimond: We use property interference at the moment, which is authorised under the Police Act. We use it for a range of purposes, ranging from pretty much every-day relatively routine activities right up to far more high end. The difficulty is that trying to describe any of those techniques in this setting probably would be inappropriate, but I would certainly be very happy to explain them in a great deal more detail if we had the opportunity to do so.

Matt Warman: More generally, in that case, how often do anticipate being required to use equipment interference in the future?

Chris Farrimond: That is quite difficult to answer, because I could not have predicted the IP revolution that there has been or the digital change that we have seen. The change from traditional telephony into IP-based communications has been enormous and the pace has been really difficult to keep up with. I could not make any prediction about just how much we would use this. I suspect that our limitation would be around our own resources and

our own capability rather than the demand. The demand for quite a lot of the services that I am allowed to manage within the NCA outstrips supply.

Keith Bristow: To give you a trend, I think it is fair to say that as law-abiding citizens it is no different—more of what we do now is online using digital devices. I imagine that the trend will peak, but I think that we will be doing more rather than less that reflects the behaviour of the criminals who we are targeting.

Richard Berry: To give a police perspective on this, we use equipment interference regularly, really for tracing vulnerable and suicidal missing persons.

The other point I would like to make is that there has to be some consideration from our perspective of the integrity of the information contained on a device that is interfered with. For example, to comply with the requirements of Section 69 of the Police and Criminal Evidence Act on the integrity of computer information, there might be considerations perhaps prohibiting the creation of data purporting to be communications data on that particular device or perhaps removing such data from that device. The evidential integrity of that device might be particularly important. Perhaps we can expand on that in a written submission.

Q38 **Matt Warman:** Finally, on demand versus supply, do your organisations currently have the capabilities technically and in terms of manpower to do what is needed? Do you anticipate seriously being able to ramp that up?

Chris Farrimond: We have the capability, and I anticipate that, if required, we could ramp it up, yes.

Keith Bristow: The change for the NCA and the transformation programme that it is going to go through—the Government announced the funding for that last year—mostly relates to our digital capabilities. As criminals go online, we need to be as adept in the digital environment as we are in the physical environment. Those capabilities are going to be invested in on behalf of the whole law enforcement community and not just us, because we provide those to our colleagues in HMRC, for instance.

Richard Berry: RUSI recommendation 5 as being that law enforcement should have a comprehensive digital investigations intelligence programme. A number of colleagues are here and we are part of that programme. Building capabilities is certainly one of those priorities.

The Chairman: Thank you very much indeed. Again, apologies for the delay because of the votes. This has been a fascinating session and we look forward to receiving your written evidence to supplement what you have told us today.

Keith Bristow: Chairman, do you mind if I just reiterate Chris's offer? We want to be open and transparent with the Committee and the public viewing this or reading the report are hugely important. However, we cannot betray all our tradecraft to criminals.

The Chairman: Of course not.

Keith Bristow: There is an open offer to the Committee, and I know that I speak for my colleagues as well; if you want to look at what we do, whether in a comms data unit or about equipment interference, we will brief you at a higher level of classification to help with your deliberations. Thank you for your time.

The Chairman: That is very generous of you. Thank you very much indeed.

Michael Atkinson, Secretary to the National Police Council's Data Communications Group (QQ 162-173)

Evidence heard in public Questions 162-173

Oral Evidence

Taken before the Joint Committee

on Wednesday 16 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Lord Butler of Brockwell, Bishop of Chester, Lord Strasburger.

Witness: **Michael Atkinson**, Secretary to the National Police Council's Data Communications Group, gave evidence.

Q162 The Chairman: A very warm welcome to all of you. I was just saying that this is a rather large room—a bit like Mussolini's waiting room, if you ever saw that. You are miles away down there. Can I say how valuable the Committee thought our visit was yesterday, by the way, as an introduction? It was extremely useful and gave us a lot of food for thought. I am going to start the first question and my colleagues will come in afterwards. Do feel free, each of you, to comment on the answers, if you so wish.

This question is very general. What is your view on the Bill? To what extent do you think it is necessary, and how will it improve and affect the operational work of your respective organisations? Do you feel it goes far enough?

> ***Michael Atkinson***: Thank you, Lord Chairman, for inviting us here today. We are pleased that yesterday was of benefit, hopefully to you all, to see how our working practices take place.
>
> Could I first introduce us? My name is Michael Atkinson. I am the secretary for the National Police Council's Data Communications Group, and I work for ACC Richard Berry, who appeared in front of you several weeks ago. To my right is Detective Superintendent Matthew Long. Matthew is a deputy head of UK operations within CEOP, which is part of the NCA. I hope that Matthew and I may be able to provide you with some evidence on our use of CD and how this relates to the Bill. On my left is Detective Superintendent Paul Hudson. Paul leads and is the head of the Metropolitan Police Service's technical surveillance unit. He will, I hope, deal with any questions you have in relation to equipment interference.

The Chairman: Thank you very much indeed. Of course, we met some of you yesterday. Anyway, what is your view of the Bill? Is it right? Is it necessary? Does it do what you want it to do, and does it go far enough for you?

Michael Atkinson: I suppose it is no good me sitting here talking to you about the change in technology. You have probably all seen enough, since you have been in this Committee, about how technology has changed. What is happening with policing? We are struggling. How are we struggling? We are struggling to keep pace with how victims, witnesses and criminals use technology. In many investigations, we try to use CD as evidence. It is causing us problems to obtain this evidence. We use CD in many investigations: theft, child sexual exploitation, homicides or frauds—a wide spectrum of offences. Our inability to obtain this data is increasing, for various reasons. Some CSPs do not retain the data for long enough in certain services. Some CSPs are outside our jurisdiction; we have difficulty with their laws in obtaining the data, and some CSPs outside our jurisdiction will not assist us. Also, some of the data is not retained. I have said that it is not retained for long enough, but the actual data that we require is not retained. We believe that this Bill will assist in closing some, but not all, of the gap that we are currently experiencing.

Paul Hudson: Lord Chairman, if I may I will also bring you the EI perspective on this. We would seek further capability. The Bill currently provides extra oversight, which we welcome, but it is all about serious crime. On very rare occasions, as I hope we demonstrated yesterday, we might use EI to protect the most vulnerable people, and that might not be in serious crime; it might be to save them from doing harm to themselves. So, in the emergency provision, we would look for something that legitimises that use of EI: to protect the most vulnerable people from harm.

Q163 Mr Hanson: Thanks for coming in. My apologies for yesterday; I was on another Select Committee elsewhere in the building. For my benefit, but also to put it on the record, it would be really useful if you could give a couple of concrete examples of how the current use of powers has led to convictions or, as you have said, has been of help in providing safety or rescue to individuals.

Michael Atkinson: Unfortunately, you were not there yesterday, because you would have been provided with evidence that clearly showed how we use communications data in protecting the vulnerable. You would have seen and had explained various examples of young missing children and people who were going to commit suicide. Unfortunately, we did not manage to save everybody.

We use the vast majority of communications data to protect the vulnerable and save people's lives. In addition to that, our use is predominantly in two areas of our business: proactive and reactive investigations. That is what we use communications data for. In proactive investigations, we may use it to identify a conspiracy and people talking to each other. We may use it to identify people's whereabouts at certain times. We also use it to identify other leads; for example, somebody may have phoned a travel agent and it gives us a lead so that we can go there. We may be able to get that information, take further steps and make further inquiries. So in proactive investigations, we use it in various ways.

In reactive investigations, the offence has predominantly taken place. Murder is probably one of the more serious crimes that we look at. My background is as an SIO, and in every murder investigation in which I have been involved we have used communications data. Why do we use it? We need to identify where the victim was and where their last movements were. It may be over a 24-hour period or it may be just a relevant period of time. We also look at and identify people with whom they have had contact and, again,

that may be over a 24-hour period or a specific time period. That is no different when we identify a suspect: we would look at their data, their locations and who they are talking to. We use it across various offences.

We use data together with forensics and other data opportunities, such as ANPR and CCTV. In 2012, we undertook some work and identified communications data use in 95% of all serious crime prosecutions. We use communications data in 100% of counterterrorist investigations. Matt will probably give you some more examples of how it is used in CEOP and its work.

Matt Long: In answer to your question, the Bill is essential and invaluable. I will give you two operational examples. First, the National Crime Agency's CEOP receives between 1,300 and 1,500 referrals every month from the National Center for Missing & Exploited Children in the US, the majority of which are reported online. Every one of those is a child at risk or a suspect for us to identify, and with the majority the starting point is the communications data. For each of those, myriad further victims or suspects may be identified who we need to follow, so in the daily, weekly and monthly movement in the National Crime Agency that is the volume that we need communication data to support.

A more personal example is that I am still the senior investigating officer for Operation Notarise. Within that operation, we arrested 745 offenders nationally. Every single one of those offenders who we arrested had a comms data application attached to them, and some had multiple applications. Within that investigation, we safeguarded over 518 children, so as the senior investigating officer I see it as a tool in the toolbox, although not the only tool; it is complemented by other tools such as open source. To summarise, there is that daily, weekly protection of children. In the large-scale and small-scale operations, we need it critically to progress.

Mr Hanson: What areas of new media are you not able to access now because of the way in which the legislation is currently framed?

Matt Long: A very simple example, which I was going to come on to later but will bring in now, because it illustrates it, is in grooming. With the grooming of a child on a communications platform that is online only, if we request that data we want to know who that child is talking to. Who is that offender? Are they talking to other offenders or children? There is some data that we simply cannot get. If that is the only route by which they are communicating, which is increasingly the case, it simply is not available to us.

Mr Hanson: What is the difference between seizing PCs and seizing mobile telephones to get that data, as opposed to having the powers under this Bill?

Matt Long: You need to have the computer or the phone to be able to do it in the first place. Our difficulty is that we may have a report that has come across from the National Center for Missing & Exploited Children, which says that a child is in communication with an individual, and we do not know where they are and do not have the devices. It is quite easy once you have the offender in custody and you can go to the device. Then we will proportionally assess those devices and see how many offenders we can identify and other routes that we can follow. Ultimately, sometimes the very first step is that communications data. Without it, we cannot take the first step, which is the identification.

Q164 Lord Strasburger: Good afternoon, gentlemen. Is accessing internet connection records, if that can be done, essential for the purposes of IP address resolution and identifying persons of interest?

Michael Atkinson: I have spent several hours in one of the UK CSPs for mobile phones. I cannot sit here and say that I am a technical person who understands the technical issues to do with how telephones are used, how they retain the data, what data they retain and what they might need to do to provide ICRs. What I can say is that they are assuring me that, without the retention of ICRs, they will not be able to solve internet protocol resolutions. They also tell me that we will not get the evidence that we need in order to undertake further investigations of people who may be of interest to us. Matt has given you one example. Another example is a terrorist investigation. We do not do live inception in all terrorist investigations that we undertake. We may do investigations for months and months, identifying intelligence, connections between people and what the suspects are intending to do. If we are investigating some suspects and have some intelligence but it is insufficient to arrest, we would like to know whether they have gone to a website on how to make a bomb, whether they have gone to a website of a major shopping place in the UK, whether they have gone to a website where they might wish to book some tickets to leave the country. Currently, we cannot get that. We believe, and we are told by the communication service providers, that ICR will solve this.

Q165 Shabana Mahmood: Last week we had oral evidence from a number of smaller CSPs, and one of the things they said on internet connection records that struck me as important was that the internet connection record would probably provide a useless bit of information. If you had a mobile telephone for a young missing child, for example, all the ICR could tell you is that that phone had been connected to Twitter or Facebook for 24 hours a day for the last six months from the point at which the phone was bought, because many of the apps that are used are automatically connected to the internet. I have just checked my phone. I have background app refresh on, which means that it is automatically connected on a 24-hour basis. Is there a danger that lots of information that you collect from internet connection records is just useless: it gives you no additional investigative assistance?

Michael Atkinson: Again, we look at what we are being told by the largest CSPs. If we have a missing person, we conduct a lot of inquiries. CD may not be our first inquiry. We have other inquiries to undertake, but we may identify that the missing person has a phone. What better way to trace them than through the cell site to identify where they are?

Sometimes phones have been turned off, but we can get back the fact that they have been talking on Twitter to somebody. Even just by getting that back, we can go to Twitter. Twitter, and not necessarily just that company but other companies, will help us to identify vulnerable missing people. They will identify to us that they may have been in contact with certain people, who would give us further lines of inquiry and may allow us to identify where this missing person is. ICR could tell us that they have booked a train ticket. They have gone to a train line; it looks as though they have booked a train ticket. We can make inquiries with them. We can see that they have. Maybe we can locate where they have gone. The CSPs that I have spoken to have made it clear that ICRs would assist us.

Shabana Mahmood: National Rail Enquiries, which is the main app that most people use for booking their train ticket, is on 24-hour background app refresh. I suppose this Bill is

introducing a whole new regime for internet connection records. My question is: is it necessary? Will it just give you oodles and oodles of useless information? If you are trying to trace a child, you know they are on Twitter and you can get into their Twitter account or ask their friends, who are more likely to be able to tell you what the Twitter or Facebook activity of that young person was.

Michael Atkinson: That is what we try to do, but there is always this issue. Matthew explained the relationship with grooming. We can get a lot of information that can assist us to identify where they are. We realise that there is collateral intrusion. We realise that there are risks to this, but on the other hand there are children and missing people. Are we willing to go further to try to save a life or to bring the person back to their family?

Stuart C McDonald: First of all, just following up on those points, in quite a lot of missing persons cases, for example, it must be pretty straightforward to establish whether the missing person has a Twitter or Facebook account and then, once you have done that, you can go to these communications service providers and find information about who they have been contacting and so on.

Michael Atkinson: Sometimes we can, yes.

Stuart C McDonald: How often are you frustrated in trying to find what people have been doing to communicate with others?

Michael Atkinson: I cannot sit here and say how often it happens. What I can say is that it does happen. Some companies will not assist us; some companies that are outside our jurisdiction will not support us and help us with identification, but many of them do.

Q166 Stuart C McDonald: Now, as you will understand, the proposal is for communication service providers to be required to retain communications data and internet connection records for 12 months. What is your comment on 12 months being the specific limit? Would you want more than that, or could you cope with six months or three months?

Michael Atkinson: It is interesting that this has come up several times. I was involved in the 2012 Bill. In 2012, we undertook a survey across policing. Sixty-four law enforcement organisations, in 2012, undertook applications for communications data. We received replies from 63 organisations. They undertook a two-week survey in every SPOC unit. The unit that you went into yesterday recorded, over a two-week period, every application that went through the unit in each of the 63 organisations. That gave us a really good breakdown of how we use communications data, but also of the history of the data that we are applying for. To give you an example, we covered nearly 10,000 pieces of data and applications. That is what this survey was about. Nine per cent of those applications were for sexual offences. What was interesting was that 37% of that 9% of data that we applied for was more than six months old. We would say, and you can see, that retaining the data for more than six months is very important. We also identified that 1% of all the data was for terrorist investigations, and 27% of that data was more than six months old. Now, I know we are writing to you, Lord Chairman, and we would be happy to provide that data to you with our submission, but it provided us with some really good background and understanding of why. Further, it shows what is more than nine months old or 12 months old, so there is more data there.

What is really interesting is a document produced by IOCCO on 20 November, only last month, which is a breakdown of communications data and applications. It shows over 100,000 communications data applications, 19% of which were in relation to sexual offences. Two things jumped straight out at me. First, this is a 100% increase from the survey that we did in 2012. Secondly, 37% of roughly 19,000 is over 7,000. We would say that, if we retain data for only six months, hundreds if not thousands of suspects for sexual offences would likely evade prosecution.

Stuart C McDonald: Can I just pick you up on that, though? That information is very useful, but it does not tell us how crucial that information is at six months old, 12 months old or whatever it is. I suspect it is almost impossible to gather that, but what is your personal view?

Michael Atkinson: We have had the conversation about when we undertake investigations. A homicide investigation is a bit like a jigsaw, but you need all the pieces to make the picture. I will have communications data. I may have CCTV. I may have forensic data. I may have ANPR. There are quite a few pieces to make up that jigsaw. What you cannot necessarily say is which piece was crucial in detecting and prosecuting that person for that offence. The whole picture helps to prosecute, not an individual piece.

Q167 Victoria Atkins: Following on from that, perhaps this is an easier way of looking at it. Is there a single serious organisation case that you have investigated and taken to trial in the last decade that has not involved mobile phone records or records of telephone communications?

Michael Atkinson: I cannot sit here, hand on heart, and say 100% that there is, but the data shows that in 2012 we used it for 95% of all serious and organised crimes. I would be very surprised if any serious and organised crime case went to court where we had not used communications data.

Matt Long: Perhaps I could elaborate further for you. I gave the example earlier of Operation Notarise, with 745 arrests and 518 children safeguarded. In that operation, within a 12-month period, we resolved 92% of data. If I had 12 months, I would get a 92% return. If that dropped to six months, I would lose six out of 10 of the pieces of data. Out of six months, we would lose 60% of that offending population. If you dropped it by a further 12 weeks, I would have lost 87% of the lines of inquiry presented to me. In that case, the first point was communication data. To answer your question about what the impact would have been on me in that operation, it would have been those percentages at those time stamps. When you think about that in relation to that operation, the majority of the offenders in that operation were not known to law enforcement. It is not as though I have another database that I can check and then identify that person by some other means. I simply cannot do that. When you think that 15% of those people were in a position of trust—they were a teacher, a scoutmaster or in another position where they were the guardians of our children—it is very unlikely that I will find another route, because those individuals have gone through criminal record checks. They have gone through the very good safeguards that we have as a country, but effectively they have beaten them. That example shows you what the output and the outcome would be if you reduced the length of retention in those ways.

Michael Atkinson: Sorry, Lord Chairman, could I just cover one other point? We do not use communications data just to prosecute people. We clearly use it also to prove that people have not committed an offence. The defence uses communications data. For our more serious cases, especially if we are talking about counterterrorism, homicides and serious and organised crime, can take six months, nine months or over a year to come to trial. If the defence serves their defence statement on us six or seven months after the offence has taken place and we only retain data for six months, it would prevent them from having a fair trial and it would prevent us from checking alibis and defence statements, so we believe that 12 months is the appropriate period.

Matt Long: Can I make one final point on that? The other thing, going back to your point, is that victims do not disclose on day one when the communications data is available to us. It may take them weeks or months to gain the confidence to disclose. Then, we do not get a consequential order of victims so that we know that A leads to B who leads to C. It might be that A leads to E, E leads to another 100, and we have to review them. All that takes time. It is not necessarily even at that first instance of the offence when we need the data. We need to conduct the investigation and be allowed sufficient time to do that. Sometimes that can take months.

Q168 **Dr Andrew Murrison:** Good afternoon, gentlemen. Twenty years ago, we did not have any of this technology available to us, so setting aside crimes that are specific to modern communications such as online paedophilia et cetera, it follows from what you have said that since you now do have access to all these investigative modalities, your clear-up rate should have been dramatically improved and your ability to secure missing people, for example, should have been improved. Is that in fact the case?

Paul Hudson: As much as we have greater technological investigative powers, the criminals we seek to arrest and bring before the courts also have greater technological ability to avoid us. We have seen that the increase in technology, the mobile nature of communication and the mobile nature of making meetings have made it more difficult. The criminal of 20 years ago used to meet at a safe house and it was a lot easier to understand how they communicated. The criminal of today tends not to do that, because they have the ability, as we all do, to communicate on the move. Our capability is merely moving with the capability of the criminals we seek to address.

Q169 **Dr Andrew Murrison:** I am not entirely satisfied by that, since you do have an increased range of ways in which you can keep tabs on criminals and investigate them, which draws me to my next point, which is on equipment interference. My first question is: in what proportion of the cases that you deal with is equipment interference used?

Paul Hudson: I do not have the percentage proportion.

Dr Andrew Murrison: What is the ballpark figure?

Paul Hudson: It would be the majority, but it would be difficult to answer in a public forum.

Dr Andrew Murrison: It is a majority of the serious crime.

Paul Hudson: It would be difficult to answer in a public forum.

Dr Andrew Murrison: That is interesting. Okay, perhaps we can come back to that. What concern do you have about the evidential nature of the material that you can generate using equipment interference? In other words, can it be admissible in court, and is it degraded in any way and thus rendered inadmissible?

Paul Hudson: The whole point of law enforcement is to gather evidence that we can place before a court—the best possible evidence. Everything we do is aimed at that. It is covert by nature, but we would not do anything that would degrade that, because when we come to trial we would have to place before the court evidence that we can adduce and provide a fair trial. Nothing we do would reduce the quality of the evidence that we are collecting.

Dr Andrew Murrison: Are you at all concerned that what you do by way of equipment interference poses a risk to wider users? Clearly what you are doing has been characterised as being legalised hacking. I know that is an awful generalisation, a bit like the snooper's charter, and we should really bin those kinds of clichés. Nevertheless, it is the way the *Daily Mail* would present it, for example. That suggests a certain amount of damage that is being done or caused—damage that, since it is associated with the state, is potentially the subject of some sort of comeback against the agencies. Have you any cases where that has happened? I suspect you would not be very happy to share them in a public forum. Are you at all worried that your capability to do this work will at some point come back and bite us?

Paul Hudson: First, I am not. Equipment interference is a covert capability, so nothing that we do under equipment interference would cause any damage or leave any trace, otherwise it would not remain covert for very long. Again, the endgame is to collect evidence to place before a court. If we were causing damage to equipment, that would reduce the ability for the evidence to be alluded to.

Dr Andrew Murrison: You are confident that your activities, by way of equipment interference, will not in particular harm innocent people and render innocent systems compromised or inoperable.

Paul Hudson: Before any deployment, a risk assessment is conducted, and that is part of the authorisation process that would be reviewed by the authorising officer. Subsequently, before authorisation is given, all those risks would be outlined for the judge or the judicial commissioners. Of course that would affect the proportionality and the collateral intrusion that would occur.

Michael Atkinson: I want to cover one thing that Paul said about the majority. We will provide some data, if required, on the use of this type of equipment. We would ask that it is not shared in relation to any reports, because it is very confidential. The other point is that I think it was quite clear, in a couple of the investigations that were shown yesterday, how important this is to us. I will not go into any more details about that.

Matt Long: On the change in crime that we have seen recently, we are starting to see victimless prosecutions, where we have the video of the rape of the child, who is a neonate, too young to talk, but we have the opportunity to use comms data to identify that and to recover that evidence. For CSE, there are very specific examples where the child is unable to report and we use that data to bring a prosecution, which we would not have been able to by any other means. The conviction data, which I am sure can be provided if requested,

shows a year-on-year increase in the responsiveness of the UK to deal earlier with indecent imagery of children across the country. In my particular area, there is a very definitive use that can be seen.

Lord Strasburger: On the evidential quality that comes from computers that have been subject to equipment interference, the other risk is that a guilty person could get off if his defence lawyer discovers that equipment interference has taken place and alleges, for example, that material was planted on the computer at that time. I can see a risk here, and I think others can too, to successful prosecution using evidence from that computer if a third party—in this case you—has had their fingers in it.

Paul Hudson: As we discussed yesterday, equipment interference does not stand alone. As already described, an investigation is a jigsaw puzzle of evidence that is placed before the court, and we would use the current judicial process under the CPIA to ensure that the judge in PII was made fully aware. We would obviously reveal all to the CPS, which would then, through the prosecution counsel, place it before the court and the judge to ensure that the judge knew exactly what had happened, how we did it and our methodology, so that he or she could take a decision on fairness. We would merely place before the court the evidence that is adduced. It would be for the judge to decide.

Q170 Lord Strasburger: Thank you. Can I just talk briefly about intercept as evidence? The lawyers in the Home Office have various views on the admissibility of intercept as evidence. It would be very interesting to hear from policemen at the coalface how helpful or not that would be for you.

Michael Atkinson: We are aware of many studies. It is not our part of the business, although we understand it and know it takes place. It is up to the people who are involved in that area of the business to decide whether they feel it should be used as evidence, and not us.

Q171 Suella Fernandes: Good afternoon. Could you describe for us the oversight and monitoring regime that regulates the process?

Paul Hudson: The majority of the current regime is under the property Act. Originally, the applicant will make an application and lay out their view on proportionality and necessity, as defined, and justification. Under the Bill that is reviewed by a chief officer, who will make a similar assessment. Then it is passed to the judicial commissioner to review and authorise. My understanding is that that is independent, which is welcome. The Act makes it a lot clearer that we have this ability to use it and that we would use it. It is more foreseeable in line with David Anderson's recommendations. Under the Police (Property) Act 1997, the intrusiveness depends on the level of intrusion by the surveillance commissioners. The less intrusive methodologies that we use are authorised and then reviewed, and for the more intrusive methodologies we have to get prior approval under the IP Bill, which is good. We welcome that.

Outside that, my understanding is that the Bill is going to bring together the three different oversight bodies, IOCCO, the OSC and the Security Committee, and make them one. They will continue in that yearly review and that regular inspection of our capability, in line with how it works today. The two different commissioners for the police come to us, look at all

our records, look at how we have deployed, what we have deployed against and have free run of all our databases. It is a much more stringent oversight for us. It is clearer and better in relation to my part of the business.

Suella Fernandes: What practical impact do you think the proposals will have on the process of getting permission to use the powers?

Paul Hudson: Personally, providing there are enough commissioners and the speed is available, there will be no real impact, and the emergency criteria also fit. As I said, it reflects the police Act, so I do not feel that there would be a lot of change.

Michael Atkinson: For CD, we would say that the oversight probably begins at the point when the SPOC becomes involved. Yesterday you heard about the role of the SPOC, and how important it is as a gatekeeper and for the advice it gives.

Suella Fernandes: Sorry to stop you there, but is the SPOC an independent person?

Michael Atkinson: They are independent of the investigation. They have a specific role within the organisation just to apply for communications data. They have first oversight of an application, and then it goes to an independent authorising officer. If it is for subscriber information, it is authorised by an inspector who again is trained and has to go through the full process to understand the application and justify whether it is proportionate and necessary. For anything else, it is a superintendent. Again, he is trained. He understands all the issues involved in making an application.

In addition, clearly we have the IOCCO inspections. These are now undertaken yearly with every force. They interview staff. They obtain some of the applications that we have submitted and review them. They may speak to the investigating officer in order to understand whether the application was submitted correctly. We consider their inspections to be challenging and robust, and we fully support them. They provide us, at times, with advice and guidance in their reports on forces. This can assist with our training. We look at the advice and guidance. We have tradecraft events throughout the year for SPOCs, SPOC managers and DPs, and we ensure that if errors and issues are identified in their reports on policing, we discuss them and look at training to improve what we are doing. We would say that the oversight is good. If the oversight was the same under the new justice commissioner, we would have no issues with that.

Q172 Matt Warman: Just following on from that, what consideration do you give to protecting innocent individuals from the impact when you are investigating people who you obviously have suspicions about? There would be some collateral damage, if you like.

Michael Atkinson: There is clearly an intrusion into somebody's private life whenever we apply for communications data, and throughout the process everybody understands that. We take access to this data very seriously. Again, you heard yesterday about the process and that the initial applicant may be a PC in a station who decides that he is dealing with a theft and the only contact that the victim had was over the phone. They may wish to, and probably will, apply for subscriber details for the person with that phone. That applicant, when he submits that document, will look at necessity and proportionality and whether the application is justified. I cannot sit here and say that they would definitely look at

collateral intrusion, but I would say that when it gets to the SPOC the SPOC will definitely look at collateral intrusion. It is the same for the DP, who will definitely look at collateral intrusion, necessity and proportionality. The gatekeepers of the SPOC will know whether we can even get this data, because it is no good putting in an application if the CSP will not even provide the data, but it happens, probably because people do not understand that some providers will not give us the data.

We have a failure rate and a refusal rate, which shows that we treat this as serious and as an intrusion into people's lives. This varies across forces, but it shows that we can refuse applications because the data is not be there but the SPOC may identify in the very early stages that it is not justified, proportionate and necessary. That can happen at that stage. The next stage is going to the DP. The DP can refuse applications. As a DP I have refused many applications. There are other courses of action that people could take. The role of a DP is not taken lightly. You understand that you are interfering with somebody's private life. I would say that the process that we have deals with those issues.

Matt Warman: Finally, once you have all this data yourselves, once it has been obtained, how do you make sure internally that that data is not vulnerable to being accessed inappropriately, either by your own people or hacked by the outside world?

Michael Atkinson: All SPOCs have PINs so that only they can access the data, which is in stores and in police organisations. Mr Bristow mentioned that no store is definitely safe, but these stores are not the same stores that our other database is on for outside access. People have to have a password to get into it. If we felt that anybody had got into this, we could go back and search who had entered, so I would say that they are very secure.

Suella Fernandes: I have a follow-up question. You talked about the test of necessity and proportionality. What factors are taken into account when you are ascertaining whether this is necessary action and is proportionate?

Michael Atkinson: For a lot of investigations, the first thing I consider is the offence. If I have a murder and I have a victim or a suspect, is it necessary? Of course it is necessary; we need to identify where that person may have been in the last 24 hours or the last two hours. Is it necessary that I need to identify who they had contact with? Yes, of course it is. That is how we conduct the investigation. Alternatively, it could be, as I have had a couple of times, somebody who had given their address over the internet or over the phone. This was several years ago, when fixed-line internet connection records—IPAR—were easier to solve. Somebody would give their address, but the first thing they were applying for was communications data. Was it necessary? You have the suspect's address. Was it proportionate? It was definitely not. Was it justified? No, you have the suspect's address; go and knock on the door. When we make these applications we take into account the offence that we are investigating and the collateral intrusion. Do I need the data for 12 hours when I am looking for my victim in an hour's period? We take all this into consideration, and that is why the process is robust and works well.

Q173 Lord Butler of Brockwell: Some of us were shocked by the use of communications data in the plebgate affair. Do you consider that use of communications data proportionate to the offence that was being examined?

Michael Atkinson: I have not been involved in the plebgate affair. I am not a Metropolitan Police officer. Without my knowing the full knowledge of the offences, what was being investigated, the level of intrusion and what they were applying for, I cannot answer that. I would need to know more information.

The Chairman: Thank you all very much for a very useful, very informative session. Thank you so much for coming along.

Andy Smith, National Union of Journalists (QQ 137-144)

Evidence heard in public Questions 137-144

Oral Evidence

Taken before the Joint Committee

on Monday 14 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Stuart C McDonald MP, Matt Warman MP, Baroness Browning , Lord Butler of Brockwell, Bishop of Chester, Lord Henley, and Lord Strasburger.

Witness: **Andy Smith**, National Union of Journalists, gave evidence.

Q137 **The Chairman**: A very warm welcome to our witnesses today. I know there was not very long notice for everyone, but thanks to all four of you for coming along to give your thoughts on what is regarded as probably one of the most significant Bills of this Session. As in previous sessions and in any similar parliamentary committee, we will ask you a number of questions, which I hope will stimulate your brain cells. We will have a dialogue with you in this particular session about the importance of privilege to the legal and journalistic professions.

I am going to start by asking a question about the legal professional privilege. How do you think the draft Bill addresses the concerns of the legal profession about privilege and the investigatory powers in England, Wales and, of course, Scotland? Does it create any new issues?

Colin Passmore: It falls to me, as the lawyer among the four of us, to see if I can address that. My name is Colin Passmore. I have been a solicitor for 31 years now and I can modestly claim to be an expert on privilege because I write the leading textbook. I am sad enough to know the thousands and thousands of cases on privilege and the hundreds and hundreds of statutes that deal with privilege. What is unique about RIPA and this Bill is that, on the face of it, they do absolutely nothing to address the concerns that the legal profession has about privilege and the way in which surveillance techniques in all their glory can be used to infringe the privilege.

Privilege, as I am sure you know, is possibly the highest right known to the law. It is over 500 years old. It is jealously guarded, not only by the legal profession but by the courts, with the result that there are usually hundreds of cases in London alone every year in which challenges to privilege are upheld. In addition, in every single statute that confers investigatory powers of any sort, whether we are talking about the police, the SFO, the Revenue, even local weights and measures departments, there is always a provision that actively protects privilege, so nobody—the police, the Revenue—has the ability to force any client to divulge their privilege. The same thing happens in statutory instruments. This draft legislation and its predecessor are unique in that there is nothing in them that protects privilege.

When this issue came before the House of Lords in the McE case from Ireland some years ago, it is fair to say that the legal profession was extremely surprised that Section 27 had the ability to enable the security services, the police and others at least to listen in to privileged communications in certain circumstances. Even the House of Lords in that case indicated a great reluctance to interpret Section 27 as giving the ability to listen in on privilege, but the House of Lords proceeded quite clearly on the basis that this happens very, very rarely. The House of Lords was at pains to say that if it happens on a regular basis there will be a chilling effect on privilege. The chilling effect is really important, because it inhibits the frankness of clients, whose right it is, with which they speak to lawyers. If that chilling effect is in play, it could undermine the right to a fair trial under Article 6, infringing on privacy rights under Article 8, and undermining the administration of justice.

We know now, from cases like the Belhaj case and other cases that have come to light in the last year, that whereas we thought this interference with privilege was very, very rare, it is happening far too often and on a routine basis. In my view and the Law Society's view, unless this legislation is amended so as to deal with privilege on its face, then privilege, this very old and supremely unique right—there is nothing else like it in any form of communication—begins to become seriously undermined.

The Chairman: Mr Musson, do you want to add anything to that?

Tim Musson: Not a great deal, Lord Chairman. My background is not legal professional privilege in the same way as Mr Passmore's. I am here to represent the Law Society of Scotland. It appears that legal professional privilege in Scotland is very similar to that in England and Wales. The differences are absolutely minimal, although it has arisen in a slightly different way. There are the two sides to the privilege: England started on one side, Scotland started on the other side, and they have come together. Certainly the Law Society of Scotland is very concerned about the erosion of legal professional privilege that appears to be quite possible with this Bill. They have great concerns about it, which do not differ in any way from what Mr Passmore was saying.

The Chairman: Picking up on where Mr Passmore finished, and now that you have added to his comments, it is very appropriate for our only Scottish member to come in on the issue of any possible amendments.

Q138 Stuart C McDonald: Mr Passmore, you suggested that this Bill will need some amendments before you are happy with its approach to privilege. Can you give us any more indication of what sort of amendments you think would be required?

Colin Passmore: There is a serious question as to whether there should be a prohibition on interference with privilege at all. Why is this interference necessary? I respectfully suggest that there are not many cases where lawyers, be they solicitors, barristers, advocates, have been found guilty of abusing the privilege. If a solicitor or a client in their relationship with a solicitor abuses the privilege, the privilege falls away. There is something known as the crime-fraud exception or the iniquity exception.

You do not need these seemingly open powers to listen in to solicitor-client conversations unless you have some evidence that there is something wrong going on. There is very little evidence that solicitors or lawyers abuse the privilege, and therefore the power to listen

in, to intercept or to hack is simply, in my view, unnecessary. I would be a strong advocate, and the Law Society is a strong advocate, joined by Scotland and indeed other jurisdictions, for having the type of privilege preservation clause that you find in all other statutes, including those that deal with police powers, revenue powers and so forth. I respectfully suggest that there needs to be a provision in here that makes it clear privilege is out of court.

Stuart C McDonald: Are you frustrated, then, that sometimes we hear from the Home Office that they are scared of putting some kind of prohibition on intercepting legal privilege because of the risk of abuse? You are saying to us in effect that that abuse means that the privilege no longer applies.

Colin Passmore: That is my view. I know many lawyers who understand the importance of privilege and its unique status as a means of privacy in communications with clients. Many lawyers whom I know take the obligations that arise from having the benefits of privilege very seriously. I can think of a handful of cases in which privilege has been abused; I am aware of one, which came to my attention this morning, that has just gone up to the European Court of Human Rights. It simply, in my view, does not happen that lawyers abuse the privilege.

Stuart C McDonald: Mr Musson, do you also seek that prohibition in the Bill?

Tim Musson: Ideally, yes, I would seek that. If it cannot be taken as far as that, there become issues about who is competent to permit interception of these communications. It would need to be someone who understands legal professional privilege, and the sort of person involved in this authorisation might not have that knowledge or understanding.

Q139 Lord Butler of Brockwell: Mr Passmore is making the case for prohibition on the grounds that privilege falls away if a lawyer is engaged in criminal activity. In those cases, you would say that there must be evidence that that is happening, but then you are putting too much power in the hands of the authorities, are you not? They say, "We have evidence"—let us say this is the Home Secretary—"and, therefore, please may we have a warrant to listen to this lawyer because we think privilege has fallen away?". Would you not rather have a stronger safeguard than that, a formal procedure that certifies that that is the case, rather than just the judgment of the Executive?

Colin Passmore: That is a good point. I do not make the case just on the basis of the iniquities exception. I make the case primarily on the sheer importance to the administration of justice of the privilege itself. I am very concerned that this Bill has the ability to undermine privilege more generally. With regard to your second point, in the way this iniquity exception works with, for example, the police, the SFO or the Revenue authorities, when they seek a warrant to go into a solicitor's office, they have to satisfy the judge in the Crown Court that there is a really good case for being able to go into the solicitor's office, knock on the door and start to take papers away.

Forgive me, I am going slightly off your point but I will come back to it. If privileged materials are identified, whether or not the exception applies there is always an independent lawyer in attendance who will do the physical bagging up of the documents or the computer disks, and he or she will later go away to determine whether they are privileged. There should be

a check, of course, but a judge is more than capable of looking at the evidence as to whether or not the iniquity exception is likely to apply. Judges are very good at this.

Lord Butler of Brockwell: Would that not be covered by the new procedure under this Act: that if the Home Secretary is to grant a warrant, it has to be endorsed by a judge?

Colin Passmore: Yes, as long as the reference to the judicial review standard is removed—first, because that introduces an element of ambiguity: what is the judicial review standard? I know that eminent lawyers such as David Pannick have written to say that it is fine; I know many others who disagree with that. But I am not even sure why we need that. If the communication that the authorities wish to intercept is subject to the iniquity exception, that of itself should be enough; we do not need a judicial review standard. Does the exception apply prima facie or does it not? If a judge is not happy that the exception applies, the warrant or the ability to intercept simply should not be granted.

Lord Butler of Brockwell: That, if I may say so, raises a slightly different point. I am not trying to put words in your mouth, but I think you are saying that if the judicial review test was removed, you would be content with a procedure whereby the Home Secretary can grant a warrant, provided it is endorsed by a judge, if there is a really good case?

Colin Passmore: Coupled with an express recognition in the draft Bill, in the statute, that privileged material is not available, that would be great. I would be happy with that and I think the Law Society would be.

Bishop of Chester: The closest parallel might be a confessional and a priest. It is humorous on one level but serious on another. It is on a much lower level than legal privilege, but what qualification there is to an iniquity exception is a matter of contemporary discussion. It may apply only to the Church of England, but we have other religious groups in our country now. I would have thought that if we are going to put something in the Bill, in principle we should, I suggest, at least look at whether that is a parallel set of circumstances, because putting a bugging device in a confessional situation raises the same sort of issues in a different context.

Colin Passmore: It does. I am sorry to disappoint you, but the law addresses privilege as a higher right capable of greater protection than the confessional box. It is easier to get disclosure of your conversations with a confessor than it is my conversations with my client. I am not saying it is very easy; it is very difficult, but I am afraid privilege is on a slightly higher plane so far as the English and Scottish courts are concerned.

Victoria Atkins: To clarify, on the point of the iniquity exception, your evidence is that you wish protection to be put into the Bill that reflects the law as it stands currently across all other statutes, so if a solicitor is trying to commit a crime with their client, that information will not be protected by privilege?

Colin Passmore: Absolutely right. It cannot be protected.

Victoria Atkins: You gave the example of search warrants. Interception warrants are a much rarer event even than the pretty rare event of HMRC or whoever going into a lawyer's office. The safeguards are there, surely, for interception warrants, given how rarely, particularly in secure environments and so on, these are used.

Colin Passmore: The occasions that we know of when cases in which the police have sought interception warrants have come before the courts are relatively rare, and you have to go through the Crown Court judge warrant procedure and satisfy the judge that the iniquity exception is likely to apply. I am a long way from being an expert on interception and the security services, but I have been slightly horrified this year at the number of cases, starting with Belhaj and others, that have come before the IPT in which these issues are raised. I am not myself convinced, although I am not an expert—far from it—that these cases are such a rarity. I would therefore far rather the security services et al had in the Bill the clear recognition of just how important privilege is, plus the mechanism of going via the judge.

Q140 Suella Fernandes: Thank you for your evidence today. Do you agree that someone who belongs to one of these professions that we are talking about, maybe the legal profession or the journalistic profession, may also, albeit in rare cases, pose a threat to national security, and in those cases it is important that the agencies have a power to intercept their communications?

Colin Passmore: I find it difficult to think of a case that would be any more than a rarity. I am aware of one case in Northern Ireland, which is the case I alluded to earlier that has just gone up to the European Court of Human Rights, where a solicitor conspired with his alleged terrorist client to bump off a witness. That is incredibly rare. It is so rare it is shocking. I am not aware of any cases where that is likely to happen. I am not suggesting for a moment that every single member of the legal profession in the UK is beyond reproach—of course not—but I find that a difficult concept to get my head around.

Suella Fernandes: Do you appreciate that the agencies have given evidence that they would never specifically seek to acquire privileged material except when they apply for a specific warrant?

Colin Passmore: I would give you the lawyer's answer to that, inevitably, which is that if that is the case, they cannot have a problem with the Bill recognising the importance of privilege. In other words, if they recognise that they do not want privilege, let us put it in here and make sure it is beyond doubt. Then, if there is a circumstance in which the iniquity exception applies, go to your judge for your warrant. If your evidence is good enough, fine, you are up and running.

Suella Fernandes: Lastly, it is always subject to the test of being necessary and proportionate and that the intelligence cannot be obtained in a less intrusive way.

Colin Passmore: That I disagree with. The courts and some very famous names in the judiciary, such as Lord Denning—I am showing my age—and others since have recognised that the consequence of a claim to privilege is that the court, the Revenue and the police are deprived of what they regard as potentially relevant evidence. It is a consequence that we have to face with an assertion of privilege.

Bob Satchwell: I think your question was: could it be possible? It would be foolhardy of me to say that it was impossible, but it would be astonishing. There are so many examples of the way journalists understand and very carefully apply restrictions upon themselves in relation to national security issues through the DSMA committee, through what were

wrongly called D-notices, and things like that. We work like that all the time. I have never known of a journalist who would ever have put someone's life or national security at risk inadvertently. What we are concerned about is precisely the point that there need to be very clear procedures and rules if someone is seeking to invade the journalist's activities and his sources. More recently, and perhaps we will come on to this, the evidence has been that some organisations rode roughshod over something that we all thought was accepted.

Q141 Victoria Atkins: What is the legal status of the codes of practice under RIPA?

Colin Passmore: Vague. They are the worst option for dealing with this issue, in our view. We have a problem here at the moment in that the codes of practice that will be developed pursuant to this are so far unwritten, although I imagine they are going to reflect a lot of what is in the present codes. A code of practice is what it says on the tin: it is a code. We have seen from recent cases where the security services have breached the code that there is not really a sanction. There may be some disciplinary sanctions, but we have seen that the remedies available in the ITP are pretty low-key compared with what one might expect to get, for example, in the High Court, where there might be a claim arising out of a breach.

They are clearly not of the status of legislation. In the absence of something in the Bill, something in the Act to be, that makes the status of privilege clear, the code of practice is always going to suffer, in our view, from this weakness that cannot be cured, no matter what you put in it. It is a code. It is slightly better than the *Highway Code*.

Victoria Atkins: Should we not separate between security services and law enforcement on this issue? As you know, under the codes of practice for the Police and Criminal Evidence Act, there are very real ramifications for the prosecution if the police fail to follow the code. The case may be dropped.

Colin Passmore: I totally agree, but the big difference is that the Police and Criminal Evidence Act, or the Criminal Justice Act for the SFO, makes it clear that privilege is untouchable. You have this primary legislative direction that we do not have here, nor with RIPA. Therefore, the codes of practice are bound to suffer from that. The codes of practice currently have all lovely things about privilege, but they are effectively unenforceable. You have to trust the operatives in the security services to make sure that they will obey them and that they will adhere to them. Personally, I do not think that is good enough when we are dealing with privilege, which as I keep saying is this extraordinary right, which should be protected in the primarily legislation.

Victoria Atkins: What do you expect to be contained in the codes of practice issued under this Bill?

Colin Passmore: That depends what is in the Bill. I would like to see in the Bill: a recognition that privilege is untouchable and that therefore there should be a fair amount of guidance to the security services and others on what privilege is, why it is so important and what the consequences are of coming across it: a very clear statement, if I may suggest, that there is no basis whatsoever for targeting it deliberately; a very clear explanation of what the iniquity exception should be; and a very, very clear statement of the dangers of playing fast and loose with privilege. You may ultimately cause a trial to be stayed because you have interfered with a defendant's right to a fair trial; you have interfered with his or her

privilege. There would need to be a lot, in my view, in the code of practice. I do believe that it has to emanate from the primary direction in the Bill as to the importance of privilege.

Victoria Atkins: I have a final question on that. The commissioners will play a very important role under the draft Bill as it stands at the moment. Is it not sufficient to trust them with bearing that very much in mind when they are looking at individual applications, and in due course reviewing how the legislation is being applied generally?

Colin Passmore: The intent of the legislation is that there would be a senior judicial officer, at least at Court of Appeal level or above, so really senior, experienced lawyers. Provided they also have the direction in here that privilege is untouchable unless the iniquity exception is in play, I would be happy with that.

The Chairman: Thank you very much. We turn now to journalistic provision and privilege, touched on Clause 61 of the Bill.

Q142 Suella Fernandes: Clause 61 requires that a judicial commissioner approves the issuing of any warrants for obtention by agencies. What is your view of that safeguard in protecting the media's rights?

Bob Satchwell: Our simple view is that it does not go far enough. Some interim measures have been put in place to do with RIPA and so on, but the difficulty is that RIPA was used—I have always argued that it was misused, actually—in certain cases, some of which became very full of headlines and so on, to get around the good safeguards that are in PACE. A number of examples that learned lawyers have come up with—I am not a lawyer, by the way—show that that happened.

The key point with legislation of this kind is that we know what the basic intention is in these troubled times, but that is why legislation was enacted previously. I remember when RIPA was enacted it was made clear to me by Ministers whom I talked to, and I believe it was the will of Parliament, that RIPA was supposed to be an Act to do with fighting terrorism. We have found that, in fact, it became something completely different.

I start by saying that it is very important that the legislation—with all due respect to those who may have been involved in that legislation originally; no one expected that it would be misused in the way it came to be misused—is very clear what the ground rules are before you even get to the codes of practice. Codes of practice are fine so long as someone follows those codes of practice. It absolutely needs to understand, as most people understand—it is something I have always had in my mind, and I have been 40 years a journalist—the first rule of journalism: that you protect your sources. That is in other parts of legislation. It is understood in Europe. It is understood in most places. Judges will very rarely make a journalist reveal his sources, and so on. That background has been totally misunderstood by the police for example, who have ridden roughshod over those principles. Somehow it has to be there very, very clearly.

Going back to your previous question about the possibility of a journalist being involved in something that was against the national interest, they have to come up with evidence, not a fishing expedition; it has to go before a judicial authority. What is more, there has to be

an opportunity for the media organisation to argue and to explain the case, because it is not just a matter of delving into journalist records or into who those sources are.

An inquiry into certain parts of a journalist's activity may inadvertently reveal a source that the police or the security services are not interested in. That is why it is very important that there is an opportunity to know when the police or the security services are asking for that, and an ability to argue that case.

The Chairman: Mr Smith, do you want to comment?

Andy Smith: Yes, just to pick up and elaborate on a couple of things that Bob has said. The NUJ agrees that, while not ideal, the provision under PACE is one that we have been able to work with. We have been able not only to oppose some applications outright but to use the knowledge that we have as journalists to explain the situation that we are in, so that a judge can make a variation of something in front of him, which, as far as I can see, is very difficult under the framework that you have in front of you. A police force may come and ask for hundreds of hours of video tape and end up with 10 or 15 seconds that the judge considers to be pertinent to the application they have made.

To be clear, what we have under PACE, as Bob said, is: prior notification, which we think is absolutely essential; sufficient information about the application, for instance what other means have been attempted to obtain the information, so that we are treated not as a first resort but as a last resort; the importance of a face-to-face hearing, which is not about journalists having their day in court but about being able to demonstrate, particularly to potential sources of information, that the journalist's commitment to protect their sources goes up to defending them in open court and going to bat on their behalf; and a rigorous right to appeal before approval is granted. Under the draft legislation, there is an ability for the force or body making the application to appeal, but there is no right to appeal for any of the persons affected, simply because they are not told.

The only other point I would make initially is on the business of communications data, as opposed to the information contained in the communication itself. Journalists are in a very particular position, in that very often the information gathered has already been published and the most important thing is the fact of the communication. The communications data is at least as important as the content of the communication, quite possibly even more so, given our commitment to protect journalistic sources. It is a very particular situation that journalists are in in that respect.

Suella Fernandes: I have one final question. Special protection requires special responsibility, and in some professions the communications between the professional and their client are very well-regulated, for example the medical profession or the legal profession. There are regulations covering journalists, but they are very different from the regulations that apply to the other professions. Do you agree with that?

Bob Satchwell: Yes. It is quite reasonable. Journalism is not a profession in the sense that the professions are professions. It is not a closed shop in that sense.

The Committee suspended for a Division in the House.

Bob Satchwell: But I hope that we always act professionally, which is somewhat different. In all the codes of practice that journalists have, whether for newspapers and magazines or in broadcasting and so on, there is a simple recognition that the protection of sources is a moral duty, as it is put. That is recognised by the courts, by European authorities and so on.

Andy Smith: The other thing PACE does is concentrate on journalistic material. If a journalist, however they want to label themselves, is doing anything that is outside of that journalistic function, it is not covered. Bob talked about the times when legal privilege falls away, and, in a similar way, material that the police want to access concerning a journalist doing something other than their job would not be covered.

Suella Fernandes: The point I want to make is that there is much less regulation for journalists compared to the other professions, and the definition of a journalist is not as clear cut as it is for members of the legal or medical professions.

Bob Satchwell: That is true, but just because the regulation is not quite as formal does not mean that it is not followed. In some circumstances, the following of journalistic practice, which is accepted across the industry, is stronger because it is not laid down in legislation. The fact that it is peer judgments means that people will adhere to it.

On the question of sources and the release of information, it has been recognised in legislation and it is recognised in the courts that sources and other journalistic material should be delved into only in special circumstances.

Q143 **Matt Warman**: I should declare an interest. I am a member of the NUJ, although, I suppose, a recovering journalist. To start off with, what is a journalist these days? Would you include bloggers? Would you include someone live-tweeting this Committee who is effectively a member of the public? Where might we draw that line?

Andy Smith: To go back to what you were saying, there is an interesting debate to be had on that. I have seen various definitions. The advantage of PACE is that it does not define a journalist, and in some ways that is safer. If that definition is to develop as the technology develops, I would rather see that debate happen as a matter of developing case law, which would involve open hearings rather than conversations behind closed doors that make decisions arbitrarily, or not arbitrarily, about whether somebody who, for instance, had a regular blog and followed our own code of practice but was not paid for it would be described as a journalist. Frankly, some very good journalistic work is being done on the internet by people who are not associated with the traditional media outlets. There is a debate to be had there, but I would say it is developing.

Bob Satchwell: There are probably some common-sense definitions. It is difficult to define now, but, as Andy said, it will be developed in law. That is one of the reasons why there needs to be an ability to argue a case and say whether this person is a journalist or not. That is part of the principle that is there. I can see that some authorities would say, "We did not know he was a journalist. We just did it". That is the difficulty: that people will try to go outside what has been accepted practice in the past. It would be difficult to define absolutely what a journalist is.

Matt Warman: Bearing in mind that as-yet-undefined elasticity, how could we amend the Bill in front of us to achieve some of the things that you are talking about?

Bob Satchwell: There will be a submission from the Media Lawyers Association, which will come back in huge detail on this. Please excuse me for not having all that legal background. They will come up with some very clear suggestions on that.

Matt Warman: Mr Smith, did you want to add anything to that?

Andy Smith: Like Bob, I am not a lawyer. I would not want to start amending it for you, but the principles would involve something like "somebody who is regularly practising" or "employed". Those sorts of phrases would allow you to separate out those who are simply expressing an opinion on a blog on a regular basis from those who are engaged in journalism.

Q144 Mr David Hanson: Could you comment on what happens when a journalist is undercover and is acting as a journalist but is not, to the public knowledge, acting as a journalist at that particular time? The fake sheikh has been mentioned, but there may be other examples that we are aware of. I am interested, again, in the definition in relation to the Bill.

Bob Satchwell: In most cases, they will be employed or commissioned to be doing something undercover, and there will be some governance surrounding that from the person who has hired or commissioned them to do it. There are some difficulties if people are just going off on their own and doing it—difficulties for themselves, indeed—and they do not have the protection of an organisation behind them. That is what normally happens.

Andy Smith: The NUJ code of conduct is very clear in stating that investigations should be done by open means wherever possible and that any subterfuge has to be justified in terms of an overarching public interest, so you cannot simply decide to go away and pretend not to be a journalist because you feel that it will be the easiest way to get hold of the information.

Bob Satchwell: It is covered by virtually all codes across the media that you have to have a very good reason for subterfuge. In the new editors' code at IPSO, it is very clear that there is governance on that: at every stage of involvement in an investigation of that kind, notes have to be taken at the time about what the public interest was. It will be recorded and they will be audited on that.

The Chairman: Thank you, all four of you, very much indeed. It was very informative and very useful, and the Committee will be looking carefully at the written evidence that you will be providing us as well.

Alan Wardle, Head of Policy and Public Affairs, NSPCC (QQ 197-206)

Evidence heard in public Questions 197-206

Oral Evidence

Taken before the Joint Committee

on Monday 21 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Suella Fernandes MP, David Hanson MP, Shabana Mahmood MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Lord Hart of Chilton, and Lord Strasburger.

Witness: **Alan Wardle**, Head of Policy and Public Affairs, NSPCC, gave evidence.

Q197 The Chairman: A very warm welcome to all three of you. Thank you so much for coming along so close to Christmas. We are very grateful. As you probably know, the way the Committee operates is that we will ask you a number questions, which we hope will give you the opportunity to make whatever points you want. I will open by asking you a very general question and in each of your replies please feel free to make anything you like by way of an opening statement. What do you think of the draft Bill? Do you think it strikes the right balance between safeguarding our civil liberties and crime prevention? Perhaps we can start with you, Ms Griffin.

Rachel Griffin: I should start by saying that I am from the Suzy Lamplugh Trust. We run the National Stalking Helpline. A large proportion of the people who we help each year are affected by digitally-assisted stalking of some kind or another. The first thing to say about the draft Bill is that it is definitely necessary, from our point of view, for the police to have access to communications data to investigate many cases of stalking and cyberstalking. It is certainly necessary for the police to be able to access communications data to investigate and detect crimes. However, the point we want to make is that legislation should be only one part of a strategic plan to address digital offending. On a day-to-day basis we are finding that the police often do not make very good use of the legislation that they already have available to them. Our question would be whether a change in legislation would have an impact on the experience of victims on a day-to-day basis. On whether the Bill strikes the right balance between safeguarding and civil liberties, I defer to other organisations to answer that question. Our point of view is very much on the experience of victims of stalking.

The Chairman: That is what we would expect it to be.

Rachel Logan: Amnesty very much welcomes the opportunity to be here. We very much welcome having a draft Bill of some kind, because we are one of those organisations that has been saying for a long time that the existing statutory framework in this area is not up to scratch. Unfortunately, we are very disappointed by what we see in the Bill that has been put forward. To touch on a very small number of areas, given the time available, first, we see in the Bill not one, not two, but five sections dealing with bulk, indiscriminate collection

of or interference with individual privacy. From our perspective, that simply does not strike the balance or draw the line in the right place. We even see some targeted powers shading into what we would see as bulk powers in the case of thematic warrants.

I move on to intelligence sharing, which we have been litigating on for more than 18 months in the Investigatory Powers Tribunal. It has been the subject of at least two rulings. We were very surprised to see in what bare terms it is dealt with in the Bill, given how big the subject area is. We would have liked to have seen a clear, accessible framework, dealing with how material is received and sent overseas outside the MLATs. We would have liked to have seen that limit and not include the product of bulk interception either way—going from the UK or coming into the UK.

On oversight and judicial authorisation, unfortunately, we are disappointed by the judicial authorisation, or judicial review process, as it is put in the draft Bill. It does not amount to proper, independent judicial authorisation as is required for human rights compliance. It is simply not there. On the oversight provisions, similarly, having been through the IPT—I hope that I will get the opportunity to expand on this—we are very disappointed to see only one real substantive change to the way the Investigatory Powers Tribunal does its job. We would have liked to have seen a much more thorough look at how that works and whether it is properly independent and effective.

Finally, to touch on special protections in the Bill, again, this is an area that Amnesty has been litigating on in terms of legal professional privilege in the Investigatory Powers Tribunal, where we saw a concession by the Government that their entire regime in this area had not been human rights compliant. We saw a further finding that one of our co-claimants' legally professionally privileged material had been unlawfully retained. It is very disappointing to see nothing on the face of the Bill to deal with that properly, to deal with journalists, or even to consider giving further protections to human rights NGOs, such as ourselves, who we now know have, disappointingly, been specifically targeted for surveillance by the state. With all of that in mind, and there are many other areas that we simply do not have time to get into at this stage with the time allowed for the Bill process, we are very disappointed with what we have been presented with.

The Chairman: Thank you very much. Of course, every organisation, including yours, is very much entitled and welcomed by us to submit written evidence in detail.

Rachel Logan: We have done, this morning, for which we are grateful.

Alan Wardle: Good afternoon. Another fact that is relevant for this is that the NSPCC runs ChildLine, which you will all be aware of. It is now in its 30th year. Increasingly, children, as the Committee will know, are leading their lives online. More than three-quarters of 12 to 15 year-olds have access to a smartphone. That also means that many of the crimes committed against children increasingly have an online element. In particular, some of the ones I want to focus on are what you might call the harder-end cases, such as the possession, distribution and manufacturing of child abuse images, so-called child pornography, which is growing, and also cases of grooming of children, much of which is done online. More than 500 children contacted ChildLine last year about grooming and more than 80% of those cases had an online element to it.

From our perspective on the Bill, the most important thing for us is to ensure that the police have the powers that they need to track, investigate and prosecute these offenders. We are coming from a different place from Amnesty, which is more about bulk surveillance; we are more focused on specific criminal investigations that the police need to undertake. We have a particular concern that Clause 47 might be restricting too much the police's ability to investigate in what can be quite complex investigations.

Another point I want to make is that ChildLine has a very high level of confidentiality, but it has to breach children's confidentiality around 10 times a day, generally because those children are actively suicidal. Most children contact ChildLine online these days, so we need to ensure police can get those IP addresses quickly and actively intervene to protect those children. The two aspects that I would like to talk about are criminal investigations and ensuring police have powers, and an emergency function to protect a child's life if they are in immediate danger.

The Chairman: Thank you, all three of you, very much indeed for those opening remarks.

Q198 **Mr David Hanson:** The police's case, as put to us by Keith Bristow of the National Crime Agency, is that the Bill brings us up to speed with "what we need to be able to do in a digital age compared to an analogue age". Do you agree with that, or do you think the Bill goes further and adds new powers for the police?

Rachel Griffin: I smiled because I can see why that statement was made in theory, and it might well apply to cases of, for example, child sexual exploitation, where the focus is on intervention and stopping criminal activity escalating. From a stalking point of view, the key use of communications data in cases that we deal with is on investigation and detection in individual cases where the activity has already happened. We tend to find that it is not so much a case of whether the police have the powers; they already have a number of powers but we find that they simply are not being used in practice. For example, we often hear from victims of stalking who have been told to turn off their computer—"If you don't look at the emails it won't affect you"—or they might be told that that it is too expensive to investigate digitally, or that there is no point as the service providers will not be compliant, et cetera. For example, recently the helpline report was told that police access phone records only in cases of murder. There is a huge gap between what is going on in practice with regard to making use of existing powers and what may be envisaged in terms of the potential of the Bill. That is why we would like to see the police using their current powers to full capacity, as is reasonable and proportionate, but also to focus on not just legislation but the capability and capacity of police forces to make use of that legislation.

Rachel Logan: I will leave this to my colleagues at this stage.

Alan Wardle: The police's view on powers is quite important. From our perspective, we understand from the NCA that there has been a gradual erosion of the amount of data that they have been able to gather over the years. The Bill is very important to put that in place and to ensure that it is adaptable. Who knows what technologies there will be in five to 10 years' time, but the Bill has to have sufficient flexibility to adapt to those things.

On Clause 47(4), which has additional restrictions on granting authorisation, we have had initial conversations with the police and they have expressed concern about it. It would

seem to us perverse if the data providers were able to hold all the information but the police were unable to access it. My understanding is that if people were conspiring over the telephone the police would be able to have all that information, but not if it was done online. That subsection talks about where the activity is mainly or wholly acquiring material the possession of which is a crime. Something such as possessing child abuse images is clearly a crime, but we know that for grooming cases where a lot of people are involved and it takes a long period of time, where, for example, a person books a hire car in place A and drives to place B or they book a flight, those factual issues, while not a crime in themselves, can help the police to investigate. It would be worrying to us if anything restricted the police's ability to investigate thoroughly along all the different strands of investigations. We would want to ensure that there is parity across the board and that the data the providers hold can be accessed by the police force for specific investigations.

Mr David Hanson: The question to all of you is: are the police powers under existing legislation proportionate and effective? Will they be more proportionate and effective under the proposed Bill, or will they be neutral or less effective? What is your view as to the police-central cases: do we need the Bill to update what we currently do? Is that right?

Alan Wardle: Yes it is, but my understanding is that this clause in particular would place a restriction on them that is not currently there. That would need to be worked through to see why it has been put in there and whether it will actively hinder the police's investigation of the kind of complex cases that I am talking about: the production of child abuse images, which, again, are quite often done by conspiracies, and online grooming. Yes, the need to have these additional powers is quite clear.

Rachel Logan: I am afraid that the question of police powers is not something that Amnesty can assist the Committee with at this point. It is not a part of the Bill that we have assessed or been involved with to date.

Mr David Hanson: With due respect I think that that is copping out of an answer. If the Bill goes forward, is Amnesty satisfied that the current proposals by the police are modernising their view based on the Bill? Ultimately it is about police powers and whether they are effective and proportionate. Surely Amnesty has a view on that.

Rachel Logan: With respect, it may be seen as copping out, but we are talking about a Bill of many hundreds of pages and many parts. Amnesty is a worldwide movement that focuses on many different aspects. We simply have not assessed those parts of the Bill yet.

Mr David Hanson: So you do not have a view on whether these current proposals are proportionate and effective.

Rachel Logan: At this point I do not have a view that I can assist the Committee with on the police powers in those parts of the Bill. I can help you, as much as Amnesty can, with questions of necessity and proportionality around bulk interception warrants, the structures around targeted warrants, and what is in the Bill on intelligence sharing, but I am afraid that the question of police powers and dealing with crime simply is not something I can help you with.

Mr David Hanson: Ultimately those are police powers. The question is whether they are proportionate and effective in relation to what the Bill proposes.

Rachel Logan: I am afraid that this simply is not something that we can assist you with. Those parts of the Bill go into Parts 3, 4 and 5. There are multiple parts of the Bill. We have not had a significant amount of time and they are not core areas of focus for us at this point.

Mr David Hanson: May I respectfully suggest that, when the Bill comes before both Houses of Parliament we would want a view on those issues? They are central to the Bill.

Rachel Logan: It may well be that, when we have had considerably more time and when the Bill goes through the proper processes, we will turn to that. I simply cannot say at this stage whether that will be Amnesty's focus.

Rachel Griffin: Our view is that it is unlikely—or that we are yet to be convinced—that the Bill will have an impact on the majority of cases of stalking as we experience them. That is not because data communications are not needed, but because the expertise in digital investigation and recognising risk is not as widespread in day-to-day policing as it needs to be.

Q199 Suella Fernandes: This is a question to Rachel Griffin and Alan. Can you walk us through a typical harassment case—if there is such a thing—or a child sexual exploitation or a grooming case, and how communications data would be helpful in identifying perpetrators and securing a conviction?

Rachel Griffin: From a stalking point of view, around 70% of people who call the National Stalking Helpline report experiencing at least one form of stalking behaviour that may require police to access some kind of communications data. Some 39% have received phone calls; 30% have received emails; 36% have received texts; and 37% have experienced stalking via some kind of social networking site. It is right that you made the point that there may not be a typical case of stalking because each one would be quite different. They are incredibly diverse in how long the stalking goes on for; some will be stalked for about six months, but, sadly, we have a small proportion of people who have been stalked for a number of years.

What tends to happen is that somebody will be stalked through a blend of different means. That may include physically turning up at someone's workplace or at their home, perhaps sending them letters, but also saying things about them via social media. Some will know that they are being stalked and that the activity is taking place online, but they do not necessarily know who it is, or there is a suspect but it is very difficult for them to prove. They will go to the police and say, "This has been happening, I've been receiving these text messages, these things have been written about me on Twitter". In a case where there may have been a number of text messages or emails, the police may need to identify that it was in fact a perpetrator—an identified individual—who sent them. That is where communications data may come in. Unfortunately, that is where we have too many examples of victims saying that they have gone to the police and found that, in some cases, the police do not even understand what an IP address is. The level of understanding is relatively low. That is alongside those cases where people say, "Well, come back when he

does something", suggesting that if it happens on the internet—if the stalking is cyberstalking—it is not real stalking.

Alan Wardle: It varies in grooming. Sometimes it can be one person grooming one child, or, as we have seen in some high-profile cases, it can be gangs of people communicating with several children. The process of grooming takes time, by its very nature. It lures children in, makes them feel good about themselves, offers them enticements, et cetera. We know from the National Crime Agency that the vast majority of cases involving grooming are online. That could be through social media, by various apps, by text message, by phone et cetera. Quite often, one of the challenging things around this is that children do not even recognise that they are being groomed—they think that it is their boyfriend, for example. The child will not necessarily keep the evidence themselves; they will not hold on to it. The police need to be able to identify from all those different sources what happened, to try to get a picture of who said what to who, where they were, who they communicated with, when they did it, et cetera, to build up a picture of what is going on, which obviously would go alongside personal testimony. That is why the point that Rachel Griffin makes is valid: we also have concerns about the police's capability—particularly that of local forces—to investigate and understand these offences properly. The cornerstone to that is having the information available to them so that they can identify what has happened, build up a picture of what is going on and investigate and prosecute these crimes.

Q200 **Baroness Browning:** Are the three purposes for which law enforcement can seek internet communication records the right ones? Should they also be able to use them for other purposes—for instance to locate missing people—even when no crime is suspected? We have received evidence from the police that much of their time is taken up with trying to identify vulnerable people, not necessarily because they have fallen foul of serious crime, but speed is of the essence because they are vulnerable.

Alan Wardle: On the first part of your question, as I mentioned, certainly on Clause 47(4)(c), which is the limitation where a person is "making available, or acquiring, material whose possession is a crime"; at first glance, and having had an initial discussion with the NCA, we are concerned that that might be too limiting. Using grooming as an example again, hiring a car to transport a child from one part of the country to another is not a crime in and of itself, but it is evidence of a crime having taken place. It would be worrying to us if that data was held by internet service providers but the police could not access it because it was not illegal material. More needs to be teased out throughout the process about what that means and what limitations that will place on the police.

On the emergency bit, as I said, ChildLine has to do this about 10 times a day. We work with CEOP very closely. The ability of the police to identify and rescue actively suicidal children who may not want to be contacted by the police is a very important function. We certainly would want to ensure that that capability is not eroded in any way.

Baroness Browning: Not eroded, but as drafted, will it not add anything to resolve the problem of your 10 children a day?

Alan Wardle: I spoke to a barrister about this last week. Her initial view was that Clause 46(7)(g), "for the purpose, in an emergency, of preventing death or injury or any damage

to a person's physical or mental health", would cover this situation, but again, it would be useful for the Home Office to clarify whether, in its view, that would cover it.

Q201 Lord Strasburger: Ms Logan, you mentioned in your opening remarks that one of the five areas you are concerned about is intelligence sharing. There is very little in the Bill about it and so far the Committee has heard very little about it. Would you care to expand on what Amnesty's concerns are and what advice you would give the Committee on it?

Rachel Logan: Yes, thank you very much. Amnesty has been engaged, together with Liberty, Privacy International and several other NGOs, in litigation in the Investigatory Powers Tribunal—it will now be off in the European Court of Human Rights in Strasbourg on this subject—to look at the way the UK both sends information, intelligence product, overseas and receives it from overseas powers. In the Bill we have very little at all on what are called "overseas arrangements". Clause 39, "Interception in accordance with overseas requests", provides for that activity, but simply talks about lawful interception being something, "carried out in response to a request made in accordance with a relevant international agreement by the competent authorities of a country or territory outside the United Kingdom". The only definition you have for a "relevant international agreement" is, "an international agreement to which the United Kingdom is a party". On the other side of the coin, when we think about what the UK is requesting others to do—perhaps not requesting, but what information it might receive from other powers—all we have in the Bill is a bare reference in Schedule 6 to a "code of practice", which, it is said, will be forthcoming and which will deal with the "provision about the making of requests ('relevant overseas requests') for intercepted material or related communications data that has been obtained by an overseas authority by means of any interception", et cetera, with no definitions of what any of this might be and no expansion on what any of this might mean. There is then further provision for arrangements to be in place around receipt or sending of such information, with no explanation of whether such arrangements will be public, what they might contain or what they might be.

We were talking about the product of bulk interception, such as, in the US, the product of Prism or the upstream programmes where material has been collected in bulk. We are considering a situation where we have a ruling in the Investigatory Powers Tribunal case that recognises that, until this litigation, any such intelligence sharing was unlawful because there was no policy whatsoever in the public eye in this area. All we got during the litigation was a small summary, which was corrected on many occasions, of what the arrangements in place might be. It was very bare bones. There was lots of talk about signposting to what was under the waterline. When we were in that situation we had very much expected the Bill, in the spirit of transparency, to provide a clear legal framework. Those simple references simply do not do that. How can Parliament and the oversight bodies provide proper scrutiny? How can the public understand where their information might end up or what might be being looked at overseas if there is simply nothing there? That is very disappointing.

The Chairman: I think we will touch on that in further questions as well.

Q202 Dr Andrew Murrison: Amnesty obviously has an international perspective. I am interested in your view on whether this legislation is compatible with the direction of travel

taken by countries with which we can reasonably be compared, in particular the other four members of the "Five Eyes" community.

Rachel Logan: I want to be very careful about what I say on that topic at this point because there is a certain state of flux in the relevant "Five Eyes" countries. I would be very happy to come back to the Committee with a more detailed analysis. I will say that in the US, for example, we have recently seen, as I am sure you are aware, changes around the Patriot Act and the Freedom Act and a certain amount of rolling back, but I would not want to give the Committee any precise answers without being able to go back to that in more detail. I would be happy to do so.

Dr Andrew Murrison: It would be quite valuable if you could as part of written evidence. As we have been going through this there have been comparisons with the "Five Eyes" community, with whom, of course, we share data. It would be useful from your perspective as an international organisation to provide some insights if you could.

Rachel Logan: I will certainly see whether we can do that in the time available.

Dr Andrew Murrison: Thank you very much. May I ask you about communications data? A lot of what we have been dealing with over the past few weeks has to do with the times permitted by the Bill—for example, five days for judicial review warrants issued by the Home Secretary and 12 months for the retention of communications data. I would be interested in your thoughts on whether 12 months is right—in particular, to nuance that slightly, whether that 12 months might be amended upwards or downwards depending on the situation, on the crime that we think has been committed and on the circumstances, thinking of missing people, for example.

Rachel Griffin: We would resist offering an arbitrary time limit, which I dare say is not terribly helpful. From the National Stalking Helpline's perspective, we tend to talk to people at the very beginning of their journey through the criminal justice system. They may not even have reported the crime when they talk to us. I would advise getting evidence from people such as the CPS and the police on how long it takes for a prosecution to come to court from that point of first report. That will have an impact. It will not be terribly helpful to have a time limit that may have expired when the evidence is finally gathered and a prosecution is pursued.

Also, it is worth bearing in mind how long people have been stalked for. Some 48% of the people who talked to us have been stalked for longer than one year. That suggests that there might be a need, by the time a victim goes to the police, to go back some time to find some of the essential data. It is also really important to understand why people do not come forward, whether it is to do with cyberstalking, or, in the context of stalking, things such as revenge porn. Often people will not come forward because they do not feel that they will believed and they do not have the confidence to talk about their experiences.

Also, it is vital to point out that, in preparation for this session, we contacted the Home Office to ask how many investigations are impacted by lack of communications data—we do not know what we do not know. The feedback was that it is impossible to know how many criminal investigations are impacted by a lack of available communications data. Again, I come back to the point that we definitely recognise the need for communications

data, but we do not know the size of the problem that we are trying to solve with the Bill. Therefore, it is difficult to determine whether the existence of the data would be helpful and for how long that data would need to be kept because we do not know how many prosecutions are not going forward without that data. It feels very circular.

Dr Andrew Murrison: Where do you think the Home Office got the figure of 12 months from, then?

Rachel Griffin: I am not sure. You would have to ask the Home Office.

Alan Wardle: My understanding of the 12 months was that the last time this was legislated for Parliament took the view that that was the appropriate time. Any flexibility around that ought to be evidence-led. Certainly, we know that some of the more complex cases, some of which I have alluded to, take a long time to build up the case. We hear from the police of cases where, because it is a rigid 12 months, as the case proceeds bits of evidence fall off the end after a year. We need to know whether there is any flexibility around that once a case has started. On disclosure, again, similar to the point that Rachel made, not all children disclose immediately whether they have been abused. They can take time. It is a judgment for Parliament to make. It ought to be evidence-led and take a view on whether there are more serious and complex crimes where data need to be held for longer and how that would work.

Dr Andrew Murrison: I can see why organisations such as Suzy Lamplugh Trust and the NSPCC should want the police to have these powers since you are faced, on a day-to-day basis, with very vulnerable people. However, do you have any concerns more broadly about the acquisition and storage of communications data and potential misuse of that material?

Alan Wardle: Yes. It clearly needs to be kept safe. Another thing to remember is that children are users of data as well and they will want to have their rights and privileges protected. Clearly, there have to be very strong safeguards around that. I am not a technical expert so I would not be able to tell you how that is done, but the data needs to be kept securely. It needs to be accessed in very strict conditions to give people confidence and assurance that the data is being used properly.

Rachel Griffin: I echo that. There will be a number of cases where someone who has been stalked will have their security, whether physical or online, compromised in some way. It is critical that they have confidence that their data will be treated appropriately.

Dr Andrew Murrison: In situations such as that of TalkTalk, are you confident that there are likely to be systems in place to guarantee people's safety and security?

Rachel Griffin: Guaranteeing safety and security is very difficult. It is particularly difficult when someone is motivated by the kind of obsession and fixation that stalkers commonly display. It would be completely wrong for me to say that I would have confidence that that can be guaranteed, but victims should have a reasonable expectation that their data will be kept as securely as possible.

Q203 Lord Hart of Chilton: I must disclose to the record that 50 years ago at university I joined Amnesty International.

The Chairman: You have disclosed your age as well.

Lord Hart of Chilton: I know—how youthful I still look. We have been supplied with the open determination of the Investigatory Powers Tribunal on 22 June 2015, from which we see that GCHQ retained material for longer than permitted under the policies. Therefore, there was a breach. My first question is whether, in the light of that decision, you are confident that there are sufficient safeguards in place governing the activities of the intelligence and security agencies. I rather think from what you said at the opening that you are not.

Rachel Logan: No, indeed. First, it is important to think about what that finding tells us and then look at whether we feel that the safeguards are sufficient in the light of that. It is important to understand that Amnesty found very little out from that determination. I can come back to the question of how we got it, which sheds rather a lot of light on our views on the Investigatory Powers Tribunal, but it tells us very little at all. We do not know why our communications were intercepted and selected for examination. We do not know what was looked at and when. We do not know what policy was breached or in what way. We do not know whether this was a one-off and just confined to us, or whether it is systemic among other NGOs that were not involved in the litigation. We have had no ability whatsoever to input into the conclusions of the tribunal because we were excluded from the hearing that resulted in that determination. That begs the much more important question, as far as we are concerned, which is why human rights NGOs were being targeted for surveillance in the first place, quite aside from whether our material was retained for too long. The other NGOs in the same legal action received a simple one line, "No determination in your favour", which does not tell them whether they were intercepted, or whether they were intercepted but the tribunal considered it to be lawful, et cetera.

It is a very sparse determination, but what that tells us about the safeguards and the oversight system is that something has gone very badly wrong. It appears that this has been considered an acceptable activity by the Secretary of State and all those others involved in oversight during the process, because we know that we were picked up under a general warrant. It appears that this is something that was carrying on which either nobody raised any objection to because they all thought it was fine and dandy to be spying on human rights NGOs and did not know about the specific policy breach, or they knew about the breach and did not consider it to be important. We do not know why this was not picked up until we got into a tribunal process. It is very worrying that we had to get to that stage to get this finding.

The same applies to the other litigation we have been involved in—the legal professional privilege one I alluded to earlier—where one of our co-claimants found that his legally privileged communications had been picked up. That is a really frightening proposition for those of us who have been involved in the legal system for a long time. Again, he was not able to contribute to the hearing where the finding was made that this was not very important. From our perspective, something needed to change with that in mind. We have not seen that something in the draft Bill, particularly if you look at the retention provisions in it. Data can be retained as long as it is necessary or "likely to become necessary" to retain it. That is stunningly broad. It is very worrying for us, having been in the position of having had our data retained and having been spied on, that we do not have more safeguards in

this. I can come on to look at the IPT and the judicial relation if you would find it helpful, but basically, against that background, there does not seem to be enough.

Lord Hart of Chilton: What further safeguards do you think are necessary?

Rachel Logan: It comes back to the question of definitions. There are incredibly broad definitions around purposes in the various warrants. There is no definition of national security. Just recently, a decision by the Grand Chamber in Strasbourg, I think last week, said that it is important to have tighter definitions than just "threats to national security" when we talk about warrants of this kind. You have these very broad definitions and general purposes permitted as a basis of interception. Then you again have a complete absence of proper judicial authorisation. In Amnesty's view, this so-called double lock does not amount to a human-rights-compatible process. The decision is still being taken by the Secretary of State. It is merely being reviewed on judicial review principles by a judicial commissioner. If Clause 19(2), which states that this must be done to a judicial review standard, was not intended in any way to limit the scope of the review undertaken by the judicial commissioner, then it is unnecessary or unnecessarily complicating the situation.

Our view—like, I am sure, many of the other NGOs you have heard or will hear from—is that that is simply unnecessary if the intent is to have a full, merits-based review by an independent judicial authority before a warrant can be issued. We would like to see that happen. We would like to see strong post facto oversight done by different people than those involved in the authorisation process. This melding of the oversight and authorisation functions with the judicial commissioner is something that worries us. Down the line, looking at the Investigatory Powers Tribunal itself, I have spent nearly two years now litigating in this tribunal alongside some very well-known QCs from my old chambers and elsewhere who are well-versed in SIAC and other places where there are secret processes and unusual court systems. This court and these processes are the most frustrating and obfuscating that I have ever encountered in the UK system. We are talking about situations where, whether for intent or not—I am sure not, because everyone wishes this to be open—the bias is towards secrecy and not letting the claimant in to what is ultimately a determination of their rights and freedoms. That needs to change. All we have here is an additional right of appeal. There has been no further look at the procedures of the IPT, which allowed the Government to argue this year that, even if the tribunal made a determination to favour individuals—that they said behind closed doors, "This person's rights have been violated"—they should not have to tell the claimant. They could lie and still say, "No determination in your favour". We had a whole hearing on that topic. In the end the tribunal rejected it, but there is that level of vagueness and secrecy in the tribunal's rules. That simply has no place in a rights-compliant oversight and authorisation system.

Lord Hart of Chilton: Do you think, then, that there should be a blanket exemption for legally privileged communications?

Rachel Logan: That is the basis in English law. This is not a question merely of human rights law, this is about the common law.

Lord Hart of Chilton: No, but in respect of this Act.

Rachel Logan: Yes, we do. All there is here is a provision for codes to be available. We have to look at the safety of the justice system, as well as rights and freedoms. This is the most sensitive and the most basic principle. If I cannot, as a lawyer, say to my client that what they are telling me is entirely confidential, how can I know that they will feel free and safe and able to give me full information? There is a significant chilling effect from the mere fact of interception of legally privileged communications that really needs to be taken into consideration.

Lord Hart of Chilton: You mentioned a moment ago the Investigatory Powers Tribunal. Do you think that the provisions there are satisfactory? Again, I rather gather that you do not and that you do not think that the Investigatory Powers Tribunal provides a satisfactory route for appeal and remedy.

Rachel Logan: Indeed. The judgment we received from the Investigatory Powers Tribunal on 22 June was not in fact the final judgment in that hearing. The judgment on 22 June said, "There has been no determination in favour of Amnesty International; that is, you have not been unlawfully intercepted. There has, however, been a determination in favour of the Legal Resource Centre in South Africa—a very well-respected NGO—and the Egyptian Initiative for Personal Rights". On 1 July, having had a period for corrections and clarifications to the draft judgment, none of which were put into effect by the Government, we received an email out of the blue from the Investigatory Powers Tribunal informing us that there had been a mistake and where the judgment said EIPR, it meant Amnesty International. That was following a hearing that supposedly was looking in the most detailed consideration at our rights and at particular communications that had been intercepted and whether that was lawful and proportionate. We asked, quite rightly, "How can this happen?", and asked for an open determination explaining how a mistake of this kind had been made. We received a very unsatisfactory response from the tribunal. Indeed, Parliamentary Questions have been asked about this by quite a few Members of the House—both Houses, in fact—seeking a Statement from the Secretary of State, asking whether other human rights organisations have been in the same position, and nothing has been forthcoming. That casts light on quite how problematic the IPT currently is. It needs to be sorted out.

When it comes to the Investigatory Powers Commissioner, we set out in our written submission that it is mostly things around the edges, around independence and effectiveness. We would like to see the oversight and authorisation functions separated. This is a small group of people and they will be looking at the full process to see if it has been gone through appropriately, and reviewing that. In our view, it would be safer to separate out the functions of overseeing the process and undertaking the process, even if it is just a part of it.

Q204 Matt Warman: I would like to ask a supplementary question. Were you saying that there would be a chilling effect if legally privileged communications were intercepted? As I understand it, that power has already been avowed and therefore theoretically it is already happening and lawyers and their clients might reasonably worry about it. Has there been a chilling effect, given that this is something that could theoretically happen already?

Rachel Logan: I cannot speak for the entirety of the legal profession, I am afraid, I am simply one representative of it—and from Amnesty, obviously. It has certainly caused enormous

concern to us in how we deal with our clients. Amnesty does worldwide research and litigation on a range of human rights issues, often right at the edge of the issues that Governments are uncomfortable with; for example, looking at the involvement of our own Government in rendition and abuses during the war on terror. But we are also very much concerned with Governments overseas. It is very difficult for someone intercepting our material under a broad warrant to distinguish between what might be country research material and what might be professionally privileged because it concerns witness statements, instruction, et cetera. We are very concerned about the impact of knowing that material which is legally and professionally privileged is being picked up in their net.

Matt Warman: So has it had a chilling effect on your own communications?

Rachel Logan: I am not quite sure what you mean by that. Are we extremely concerned and worried about what we say? Yes, we are.

Matt Warman: Has that changed since the power was avowed in this country?

Rachel Logan: There is always a difference between when you worry that something is happening and when you are told that it actually is happening so, to that extent, yes.

Matt Warman: Moving on to communications services providers, from an NSPCC perspective, are you worried that communications service providers co-operate sufficiently at the moment, when information could help the kind of work that you do?

Alan Wardle: Generally, things are pretty good. Looking at issues particularly of child abuse images and how those are disseminated across the internet, Google and Microsoft—at the instigation of the Prime Minister—did some really good work a couple of years ago which means that it is much more difficult to find those images through an open search on the web. Now, with some 100,000 search terms, you get only what are called clean searches; that is, they do not give those images. So that has been good. Most of the big companies are involved with the Internet Watch Foundation. Certainly in this country we are pretty proactive so if an image is found, it is generally down within two hours, so that is pretty good.

On the content, because the majority of the big companies are American, you would have to ask the police. I am not sure how the investigation of the content of communications is working. We have an issue with some of the internet hosting companies, such as online storage functions where people are uploading and storing a whole host of images. We think that that issue needs to be looked at in more detail and we are looking at it at the moment. Most of the companies recognise that this is a very serious issue and they are generally very co-operative. It is a global issue so, while the UK is very seized of this issue, we are seeing some alarming developments in other parts of the world—such as livestreaming of child abuse, which is crowdfunded—which is why these sorts of powers are essential.

Matt Warman: Will the Bill improve that situation or not make that much of a difference?

Alan Wardle: Internet connection records are very important, as I have already indicated. When it comes to the information that is needed, the current process is often very convoluted, when you have to go through the MLAT process. Anything that could be done

to simplify and expedite that would be good. We know from the police that they do not even bother to apply for evidence in some cases because they know it will take too long.

Rachel Griffin: We have had feedback from police officers we have worked with on the National Stalking Helpline that communications service providers are not always helpful in cases where the police need their assistance. But we do not really know whether this unhelpfulness is to do with reluctance to help, misunderstanding of what help is needed, or because the legislation needs to change. What is clear is that CSPs, as well as improving co-operation with law enforcement agencies, need to provide more assistance to the victims, who are often seeking help, advice and protection after being targeted when using their services. Again, it is very difficult to say whether the proposals in the draft Bill will improve that co-operation without having a better understanding of what the barriers are perceived to be by the CSPs themselves.

Q205 **Suella Fernandes:** I have a follow-up question for Amnesty. You talked a lot about privacy rights. Obviously, we have to strike the right balance but I heard very little about national security. We have heard a lot of evidence and we have on the public record that the head of MI5 has said that we face an "unprecedented scale and character" of terror threat at the moment. We have heard from witnesses about very serious crimes that are being perpetrated online. You obviously do not feel that the draft Bill is satisfactory but where do you think the balance should be struck in meeting this very important need to safeguard the public?

Rachel Logan: There is of course a critically important need to safeguard the public. That is part of human rights protection and we all have the right to life and security and all those sorts of things. That is part of what we are looking for as an organisation. But as you say, it is a question of proportionality and where you draw the line. For example, I am sure that it would be useful for crime prevention and national security purposes if we all had to go round with a body camera on, videoing where we were at all times, and had to hand that tape over at the end of the day, or if we had to keep a list of everywhere we went and everyone we spoke to, and handed that over. That might well assist in preventing more crimes, but for most people that would be an intolerable level of intrusion into their private lives. For us, the Bill simply does not draw that line in the right place. Targeted, suspicion-based surveillance is a very different world from what is being proposed here.

Suella Fernandes: When it is necessary and proportionate.

Rachel Logan: This is the question. "Necessary and proportionate" usually means the least intrusive measure that can be used to achieve a legitimate aim. That is precisely the question that we are all here to debate and we do not think that the Bill has that line in the right place.

Suella Fernandes: My question to you, Rachel and Alan, is this. The Anderson review described Tor as a facility that enabled the digital abuse of anonymous activism and dissident activity. What is your view of this Bill's potential effect on encrypted communications in the context of your work?

Rachel Griffin: I would certainly refer you to those with greater expertise than me on the digital side of things, but my observation about encryption is that stalkers and cyberstalkers

are fixated individuals who will use any means available to them. We have had a number of cases where victims of cyberstalking have had their devices hacked by stalkers, and in those cases we have advised them to use encrypted services in future. We have experience of encryption being used for both good and bad reasons. Obviously a balance needs to be found, but I do not have the expertise in encryption to answer that question in an informed way.

Alan Wardle: Tor is a place where quite a lot of the most dedicated—if you can call them that—people who perpetrate these crimes go, particularly in the production and dissemination of child abuse images. Essentially it is a challenge for law enforcement. Being able to identify the perpetrators is very time-consuming, and I do not think that anything in the Bill will necessarily affect that. It is one of those things, given the way the internet is designed. A third of internet users across the world are children, but the internet was never designed as a child-friendly place, and we are almost going around saying, "Can you put safeguards in at the beginning?" Would you design it in this way now? I do not necessarily know that we would, but we are where we are, and certainly from our perspective the key thing, as well as power, is law enforcement dedicating the necessary resourcing and skills to get officers to do the quite painstaking work of cracking these rings of people, which are global and are perpetrating some of the vilest crimes against children. We need to ask encryption experts about that, but it is certainly challenging for law enforcement and we need to make that it has the resources—the powers, the skills, the expertise—to be able to deal with these policing challenges in the 21st century.

Suella Fernandes: I have one last question on a point that both of you raised earlier. You mentioned suicidal children getting in touch with you as well as tracking and trying to pinpoint people who are involved in stalking. Can you give us an idea of the need for timeliness in securing warrants in those situations? When you are in the process of an investigation or trying to track someone down, do you operate in a series of days and months, or is it hours and minutes that you and the law enforcement services need in order to exercise your powers?

Alan Wardle: For ChildLine it is hours and minutes. Someone will be called at 4 o'clock in the morning to breach that child's confidentiality, if that is required. There are cases of the police literally cutting down children who are found hanging and saving their lives. I was in a meeting with one of my directors not so long ago. They had to authorise something; the police intervened to protect a child who was about to jump off Tower Bridge. In those cases, it is a matter of hours and minutes, which is why there is a need for the systems that we have in place in CEOP, which are very fast and rapid. If a ChildLine counsellor and their supervisor think that the child is in immediate danger, sometimes that speed is of the essence.

Rachel Griffin: This is an excellent question, because it really helps me to draw out the distinction, as I see it, between our perspective and an organisation that is working on child exploitation. Very rarely will we deal with a victim of stalking where there is not enough risk information for the police to put protection around that victim based on a fairly well-established stalking risk assessment protocol. It is very rare—I cannot think of an example—that the information to put that protection around that victim was dependent on accessing communications data. The communications data concerns on the part of the

victims we deal with come about when evidence is being gathered to support an investigation and prosecution retrospectively. Given where stalking tends to sit in the list of priorities in a number of police forces, particularly digital stalking, which is perceived as difficult to investigate, that is where victims of stalking will end up, I fear—often at the bottom of the list of priorities.

Q206 Lord Butler of Brockwell: My final question is to Ms Logan, if I may, following up Ms Fernandes's question. Is Amnesty International opposed to bulk interference per se?

Rachel Logan: It depends on how you think about that question. Do we think that bulk interception draws the right line in the sand? Do we think it is a proportionate way of dealing with the threat? No, we do not.

Lord Butler of Brockwell: So as things are, you do not agree with bulk interception at all.

Rachel Logan: As currently laid out in the Bill, we do not consider that bulk interception—indiscriminate, suspicionless surveillance—is proportionate interference into an individual's rights.

Lord Butler of Brockwell: What needs to be done to the Bill to make it acceptable to you?

Rachel Logan: I am afraid that I can only talk to the parts of the Bill that we have assessed so far. We would like to see the provisions on bulk interception warrants stripped out. We would also like to see a change to the section dealing with so-called targeted warrants, which provides for incredibly broad thematic warrants, changed and provided with much tighter definitions. We would like to see a return to suspicion-based interference, the suspicion-based surveillance of individuals who are properly identified and properly targeted, as we would do normally in normal, day-to-day real-world life.

The Chairman: Thank you, all three of you, very much indeed. It has been a fascinating session. Thanks for coming along, and happy Christmas to you.

Adrian Gorham, O2 Telefonica (QQ 145-161)

Evidence heard in public Questions 145-161

Oral Evidence

Taken before the Joint Committee

on Monday 14 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Stuart C McDonald MP, Matt Warman MP, Baroness Browning , Lord Butler of Brockwell, Bishop of Chester, Lord Henley, and Lord Strasburger.

Witness: **Adrian Gorham**, O2 Telefonica, gave evidence.

Q145 The Chairman: A very warm welcome to all four of you. As I explained to our colleagues who came in earlier this afternoon, this is a hugely important Bill. We are very grateful to you all for coming along so that we can ask for your views about it and you can put any points to us that you wish. I am going to kick off by asking all of you how extensively the Home Office has engaged with you with respect to this Bill.

Mark Hughes: It is fair to say that Vodafone has had a number of meetings with the Home Office over an extended period. The engagement has definitely been better this time than it was in the previous Communications Data Bill period. It is also fair to say that we still have concerns over a number of aspects of the Bill, so we hope to be able to talk some of those through today.

The Chairman: Generally speaking, you are satisfied with the engagement.

Mark Hughes: Yes.

Simon Miller: Before I answer the question directly, it is probably worth emphasising how importantly we regard all our customers' data security, both in terms of keeping it safe from attack and in terms of how we process it to provide the service and experience our customers want and need, which is done strictly in accordance with law. The levels of engagement have broadly been good. They have certainly been far more extensive than anything we had experienced before from the Home Office and certainly much better than for DRIPA. The engagement has taken a number of forms—and I hope I am not speaking for everyone else here—including large roundtables with the Home Secretary, timetabled sessions and informal bilateral and multilateral meetings.

The one area that has been lacking is tripartite discussions between us as communications service providers and law enforcement agencies, together with the Home Office. It is also true to say that, although the level of engagement has been good, the iterative approach to consultation has revealed a significant number of issues with the legislative proposal that the Home Office has yet to address or has not addressed. These will be fleshed out, I am certain, in the course of this session.

The Chairman: I am sure you are right.

Jonathan Grayling: To echo that, engagement has been positive and significantly better than the Communications Data Bill. There have been some regular timetabled sessions. They have been cross-stakeholder, involving law enforcement, industry and the Home Office. That has been really useful, because it has assisted in providing a common understanding of operational requirements, technical capabilities and policy drafting. That said, this is a piece of government legislation and it is ultimately Parliament's decision what is and what is not included in the Bill. EE's main priority is our customers' privacy, and as such there are still a number of areas in the Bill that we have some concerns about, which we hope we can bring out in the next hour or so.

Adrian Gorham: I will not repeat the comments my colleagues have made, but it is certainly much better than we have seen in previous legislation that has gone through, so we are very pleased about that. We have had a good level of debate.

The Chairman: That is an interesting start.

Q146 **Lord Henley**: It is very pleasing to hear that the Home Office has been consulting, speaking as one of the various former Home Office Ministers on this Committee. We understand there is a shortage of IP addresses, and we also understand you do not always record which subscriber had which IP address and which port number at any specific time. What can you tell us about the practical difficulties and the costs that might be incurred in conducting IP resolution?

Adrian Gorham: When they developed the IPv4 standard, there were 4.3 million addresses worldwide, so that clearly was not enough, as technology took off, to give each customer an individual IP address. When the mobile phone business moved into doing internet connections, we had to come up with a solution to that, because we could not give every customer their own unique IP address. They developed a technology called network address translation, which means that every time you go on to the internet and have a data session, you are given an IP address, for a very short period, for that transaction, and then it just drops off. The next time you do something, you are allocated another one, so it is very dynamic and it changes all the time.

We had no reason to make a record of that. That is our challenge. We now need to record what number we allocate to each session and store it, and build the devices so that we can disclose that to the authorities.

Jonathan Grayling: To pick up on Mr Gorham's comments, the key point here is that at the moment the technology does not exist to be able to resolve that IP address. The public-facing IP address could have multiple thousands of unique devices attached to it. Indeed, trying to resolve that public-facing IP address to at least a near one-to-one match—and that is Parliament's intention—will require the retention of internet connection records.

As I said, the technology does not exist at the moment. We are in the feasibility stage now. At the end of that feasibility stage, it will probably take up to 18 months to deliver a solution because of the complexity involved.

Simon Miller: There is not much to add to that, other than to say that the technical challenges faced by my colleagues at both O2 and EE are replicated across the board.

Mark Hughes: I have just one thing to add. Vodafone is in exactly the same boat. We do not keep the IP data of all our customers. We are going to have to deploy new technology to be able to do this. The other thing that has not been said so far is that we will need a very big storage system to be able to keep it. It is a significant amount of storage.

Q147 Lord Butler of Brockwell: Could I take a step back and ask about the existing system and the requests you get for call data records under Sections 21 and 22 of RIPA? We know that is a diminishing resource as far as the intelligence agencies and law agencies are concerned, but are you satisfied that, to the extent you still have those records, that system works reasonably well?

Jonathan Grayling: Yes, the current acquisition arrangements under RIPA work well. One of the primary provisions, which is tried and tested, is the SPOC system. Essentially, that is the provision of comms data to law enforcement and the SIAs to a single point of contact. The use of SPOCs provides a strong, transparent and stringent process. As I said, it has been tried and tested over many years. Their SPOCs are specially trained. They are accredited in the use of CD, so they can advise their respective officers within law enforcement and the SIAs on what CD needs to be acquired.

That said, we also welcome the additional safeguards in the Bill. We welcome the requirement for a designated person, independent from the requesting agency; the streamlining of existing legislation and repeal of old legislation, so the Investigatory Powers Bill will be the primary piece of legislation for the disclosure of CD; and the restriction of ICRs to certain authorities and for certain purposes. Moving into the IP world, keeping the SPOC community and law enforcement up to speed with new technology is going to be a challenge, and a significant amount of effort will be involved in ensuring that law enforcement and SPOCs can interpret the data that we are talking about today.

Lord Butler of Brockwell: Going forward, then, into the new world—you have begun to describe the complexity to us—is it practicable, by using the internet connection records, to distinguish just the first line of the address, which is what the Government want to do, and to draw a line between that and what would be more revealing about the content?

Mark Hughes: This is where we get into some of the more technically challenging areas of the Bill, for sure. It is important that we call this out as it is. We are talking here about web browsing data when we talk about internet connection records, so we need to recognise that this is a hugely sensitive part of the capability that is looking to be developed. In terms of how easy it is, this is where we start needing to talk about over-the-top or third-party service providers, who may be running their communication services under the underlying network providers that are here today.

To try to bring this alive with an example, Vodafone and everyone else here will act very much like a postman today. We would carry a packet of data, or a letter in this scenario,

from point A to point B at an IP address. We do not know what is contained in the letter in this scenario. In future, the challenge for us is having to open that letter. Let us say it is a Skype service. We would have to say, "Okay, now we have opened it, we understand that a Skype service is being provided", and the Skype username or ID of the person would be within that. You can already start to see how the lines are being blurred between traffic data and content when you start having to open packets of data as they cross the internet.

One of the main concerns here, especially around third-party data, is that, today, Vodafone has no day-to-day business use for this data. We do not create it, so we are going to have to generate new data about our customers that we do not generate today. Secondly, we do not understand its structure. That structure can change on a day-to-day basis, and it is encrypted, so we will have to be able to strip off the electronic protection and decrypt it before we can store it. We would be concerned about attesting to the accuracy of that information as well. I am also concerned about possibly creating a single point of cyber vulnerability when you start decrypting things to be able to store them. There is a very good reason why they are encrypted in the first place. I am concerned that we will perhaps solve one problem, but not necessarily in the best way, and create another cybersecurity problem. Our point is that the very best people to keep data about the services being provided are the third parties. They should be the people who are keeping information to help law enforcement fight crime in this country, rather than the underlying service providers.

Lord Butler of Brockwell: Give me an example of what you mean by the third parties.

Mark Hughes: I gave you an example there. It could be a Skype; it could be WhatsApp. It is those types of service providers.

Lord Butler of Brockwell: I see, so the people for whom you are carrying the traffic. Okay. You have talked about this being a very complicated process. Can you give us some idea of the costs?

Mark Hughes: Until we have been served with a notice, I would be purely speculating as to the cost. I would be uncomfortable giving you any kind of idea until the Home Office has served us with a notice. It would be significant, it is fair to say.

Lord Butler of Brockwell: The Home Office produced a figure, if I remember correctly, of about £180 million. Do you think that is an overestimate or an underestimate?

Mark Hughes: Where this figure from the Home Office came from I cannot say, because we were not consulted when it was put together. We were consulted only after that figure was put together. I would not be able to speculate, from a Vodafone perspective, as to how much it would cost.

The Chairman: Would all four of you agree that the cost implications are considerable, significant, huge, something you can manage, or you do not know at this stage?

Adrian Gorham: It is going to be huge. Also, there is the way data is exploding. The increase in data is about 100% per year. That is the big issue with costs; this is going to double by

next year, with the way the internet is going. There are going to be big increases in the future, with huge amounts of data.

Jonathan Grayling: I agree. Going back to what Mr Hughes and Vodafone said, unless we can be explicit in the Bill about exactly what data we are going to be required to retain in any future data retention notices, it is simply not possible to give a figure. If there is, within the legislation, scope that third-party data falls into our areas of responsibility, the costs will be even more. We are only focusing on the data that we understand now, the data that traverses our network, the data that we require in order to route a communication and provide a service to our customers. Even then, it is incredibly difficult to come up with a cost.

Q148 Lord Butler of Brockwell: I have one final question. I get the impression that you are not enthusiastic about this provision in the legislation. You think it is a lot of work. Even if the Government meet the costs for you, you are not enthusiastic participants.

Mark Hughes: It is not necessarily about being enthusiastic. We absolutely recognise the challenge that law enforcement and Government have here. Vodafone's concerns are very much about making sure that we have a Bill that is technically workable. At the moment we are really concerned about being able to keep data about a service that is nothing to do with our core business, generating new data about our customers and especially stripping off electronic protection and decrypting communications passing through the internet. This is a highly challenging arena for any of the companies here today in which to do things on behalf of somebody else's communications services. We feel that the third parties providing those services have an obligation here to assist law enforcement fight crime.

Q149 Bishop of Chester: Clause 193 gives a series of definitions in the Bill. One of the issues we have been wrestling with is the distinction between data and content. That is in subsection (6). Are you comfortable with that distinction between data and content in the context you are describing?

Jonathan Grayling: This is an incredibly complex area and, with respect to the Home Office, it is even more complex to try to define within a piece of legislation. Without wishing to go over the ground we have just covered, there are issues in relation to what is perceived as content and what is perceived as CD with respect to who owns that data. The definitions provide a basis for further discussion. It is a starting point, and it is a starting point for defining those capabilities. That said, echoing what we have just spoken about, to a CSP, to a network provider, the communications data is the data that is available to us that we see in order to provide a service to our customers. Essentially, that is the data we need in order to route a communication that we will process and that we will make a decision on. If we do not make a decision on that data, we do not perceive that as being our data. It is simply data attached to a packet, but the data within a packet could be communications data to the sender of that packet.

Again, if you talk about WhatsApp, all we are interested in doing is sending the WhatsApp message that traverses our network to the WhatsApp server. If you were to open that WhatsApp message, you might find out to whom that message was being sent, but we have no need to know that; we are just sending it to the WhatsApp server. That data could, to WhatsApp, be perceived as communications data, but, because we have to open the

packet, it is content to us. This is where there are blurred lines and why we are looking for clarity in the Bill as to exactly what data we should be required to retain as communications service providers.

Adrian Gorham: To build on Mr Grayling's point, another issue here will be the encryption, because so much of the data now going over our networks is encrypted by those application providers. In a lot of cases, we cannot see what is contained within that traffic. They are not going to give us the keys so that we can decrypt it to examine it, so in a lot of cases we are completely blind to that traffic.

Simon Miller: The issue here is that there is a clear need for further discussion with the Home Office to arrive at a text that works. There may be a need for further interpretive text, potentially in the Bill, but there is definitely a need for more than there is currently. The introduction of the ideas in the Bill is useful, but they need further unpacking.

Bishop of Chester: Do you think your customers would make that distinction between content and data, or would they think that the data is quite personal to them, quite apart from the content?

Mark Hughes: We know that customers would expect all the companies here today to look after personal information to the highest levels possible. Concerns about decrypting third-party communications as they cross the network would be of a concern. Again, it touches on the point that the persons who should have the obligation here are the third parties. They do not need to break the encryption because they have created the communication in the first place.

Q150 **Lord Strasburger**: Putting the last two topics together, encryption and degree of difficulty, with the proportion of internet traffic that is encrypted increasing by the day, is it possible that you will end up in 18 months' time with an expensive and rather complex system to collect these internet connection records, a diminishing part of which is of any use because encryption has increased?

Jonathan Grayling: That is a real risk. Technology is moving on so quickly. New protocols, new algorithms on the internet, are being created all the time, which makes it very difficult for us to see those communications. Yes, you have encryption, but you just have the way the internet is developing in itself. I would not like to talk about timescales and I would not like to comment on the actual benefits that the technical provisions we are introducing would give to operational law enforcement and the SIAs, but it is a risk that technology is moving so quickly that we may be behind the curve.

Q151 **Baroness Browning**: The three-level categorisation of communication in the RIPA legislation has been replaced by two: entity data and events data. Do you feel that reducing these categories down to two levels causes a problem? Are they sufficiently clear and workable? Is that a good thing? Is that going to cause you problems?

Adrian Gorham: In its simplest form, it does not cause us a problem. There are going to be two types of data. There will be entity data, which is about the actual person; it will be your name, your address, your telephone number, so it is about the individual. Then there will be the events data, which describes the event and will be about where something took place, the location. The good thing about those two fields is that a different level of

authority is needed by the police if they want that data. If it is about you as an individual, that will be authorised by an inspector, and if it is the broader data that includes the location, that will be signed off by a superintendent. That gives us clarity about what is required. The challenge is that as we move forward and more and more communications are coming online and more and more machine-to-machine, there will be different fields of data and we will have to have regular discussions to find out where those fields sit.

Mark Hughes: We were clear about the previous definitions. We are not clear why it needed to change, but we have no particular objections to the proposed changes.

Baroness Browning: With the advance in technology, are you referring to the fact that things that are not in use now but are coming up over the hill are things you will have to take decisions on?

Adrian Gorham: In the future, you are going to have SIMs in your fridge and your dishwasher. All these appliances are going to have SIMs in them that provide data. That all has to go into this process, and we are going to have to make those decisions where things sit.

Q152 Mr David Hanson: It is important in this session to try to nail down in some detail what you believe the Government are trying to do and whether you can deliver it. Could you just indicate to the Committee your understanding of internet connection records, as of the Bill's description?

Mark Hughes: It goes back to what I was talking about earlier. Internet connection records are web-browsing data, so they are not the page you end up landing on but the domain that you have visited. They do not exist today, so this is about us having to create and generate entirely new data sets.

Mr David Hanson: For Vodafone, how easy is it to deliver that new data set as of today?

Mark Hughes: It is extremely difficult, because, as we have heard, the vast majority of over-the-top service provider data that would be an internet connection record is encrypted and it is not data that we understand or in a structure that we have any understanding of, because we have not created it. We are now going to have to create an entirely new type of data on behalf of another company, decrypt it and then store it ready to disclose potentially in a court of law, where we cannot even attest to the accuracy of that information. It is very difficult.

Mr David Hanson: Vodafone is an international company. What demands are being made on you by other nations outside the UK in this field at the moment?

Mark Hughes: There is no standard approach internationally. There is a real patchwork, depending on the country. There is no one model. The UK model is certainly the most transparent, but there is no one model that fits all.

Mr David Hanson: What is other colleagues' understanding of what an internet connection is?

Adrian Gorham: This still has to be clearly defined.

Mr David Hanson: The Bill is in front of us now. Is it clearly defined for you in the Bill?

Adrian Gorham: We are nearly there on the clarification of what makes up the record. The challenge is that this is something we have never kept previously. We keep your CDR for every phone call you make. We keep the record, we store it for a year, and we can disclose it. This is a completely new kind of record that we are going to be keeping, and then we have to hold it, store it and disclose it, so it is a big step up for us in what we need to do and provide.

Simon Miller: The issue here is that we know that an internet connection record is going to be something like a simplified version of a browser history, but we do not know exactly what it is going to be. Until that bit is nailed down, we cannot ascribe a cost to it or know exactly how difficult it will be to implement. We do know that it is going to stretch our existing capability many times.

Jonathan Grayling: The key point here is that an internet connection record does not currently exist and we have to create it. Even once created, it may not exist as one whole record. As Mr Gorham said, we are beginning to get some clarity on what the Home Office believes an internet connection record may be made up of, the subsets of that internet connection record. Some of that data may or may not be retained. The issue is putting it all together to try to create something that is going to be of use.

Mr David Hanson: We are the draft Bill Committee. The real Bill Committee will meet in the Commons and the Lords, probably from the end of February until the end of July, and then this will be law. The question to all of you is: are you satisfied that, by the procedure of considering this in both Houses of Parliament, the definition, the deliverability and the apportionment of cost will have received sufficient attention to have confidence among your companies and the public that it is being done to the standard the Government expect?

Mark Hughes: Until the Home Office serves us with a notice as to exactly what it wants, it is difficult to speculate. We all understand it to be web browsing; we know that it is going to be difficult and challenging and that it will create lots of new data, which is going to be highly intrusive, but until we have a notice and know exactly what we have to keep about which companies, it is difficult to speculate.

Simon Miller: There has been a process of engagement in place that has got us this far and has led to improvements in what is being proposed. That suggests that it is possible to get this over the line. However, there are still a substantive number of challenges that need to be met in order to do that. At the moment, we have not necessarily had the responses from the Home Office that we either want or need on this in order to have full faith in that process.

Mr David Hanson: Is that the general view?

Jonathan Grayling: You cannot underestimate the complexity.

Mr David Hanson: Well, let us just go back to the point that Lord Butler made earlier about the costs, again, which the Government have estimated at approximately £170 million to £180 million. We had a panel in front of us last week in another Committee room who

basically said that they estimated that they had spent £170 million, just among the two to three companies in front of us that day. Again, it is important that you, either now or before the Bill reaches deliberation stage, as well as negotiating with the Home Office, are clear about the implications in relation to the costs. The Houses of Parliament cannot pass legislation that will not be deliverable, and it is going to have burdensome costs, on the taxpayer, the public, or both. Can you give the Committee any estimate now? Could you tell the Committee, "We think it is in the ballpark figure of X"?

Mark Hughes: Again, without wishing to be evasive on this question, it depends on how much of the internet traffic the Home Office wants us to keep. Is it every single third-party service? How quickly do they want it decrypted? How much of it needs to be stored? Is it for the full 12 months, like everything else? How much resilience does it need? Do we need one set of resilience, or do we need to be able to build it three times just to make sure that it goes down? Is it that important? It is those sorts of factors that can make this change from one number to something completely different at the other end. The only thing I can say, given what we know is in the Bill and what we know about the technology in this area, is that it will be a significant cost. Saying how much it will be would be me picking an item out of the air and literally speculating. It is going to be significant.

Mr David Hanson: I take it, by the looks of agreement and nods, that that is pretty much where the panellists are. Could I just then throw the other question in, which is still an important question? Ultimately, whatever the cost is fixed at—and you have said there will be a cost—who, in your view, is responsible for the apportionment of that cost? Is it something you take as a commercial issue? Is it something the Government have to fund 100%? Where do you land on that figure?

Jonathan Grayling: We believe that the Bill should make it explicit that a company impacted by this legislation is fully able to recover the costs incurred. We believe that if there is no cap on costs based on a proportionality aspect, and the obligation and the financial impact is simply passed on to the CSP, this could result in delivering disproportionate solutions. If there is a cost recovery model that places a cap on cost and is based upon proportionality, that provides a far safer investment for taxpayers' money and the privacy of our customers.

Q153 **Mr David Hanson:** Is there any disagreement with that? No. I have one final set of questions. Ultimately, if it is doable, if it is defined, if it is delivered, and if it costs something, at some point a police officer or agency is going to ask you for information. Are you satisfied that the Bill has sufficient provision in relation to the single point of contact from officers? Is that sufficient to give your customers and you the security you believe you would need?

Jonathan Grayling: It goes back to the point that until we know exactly what data we are required to retain and the format that it is going to be stored in, it is impossible for us to say whether a SPOC or a police officer is going to be able to interpret that data, because that data does not exist at the moment. That record simply does not exist, so we cannot say whether a SPOC community is going to be able to interpret, because we do not know what they are going to be able to interpret yet.

Mark Hughes: It is fair to say that the SPOC community will have to undergo an extensive amount of retraining to be able to understand this and make use of it in a day-to-day

investigation, especially considering how quickly, sometimes, they have to be able to make a decision based on this data in grave situations.

Mr David Hanson: I will come back to the final point: this could be law, in one form or another, by September 2016. What is your assessment of the deliverability, as of today, of the Bill as it stands?

Adrian Gorham: We would all accept that this is a big step up in capability. Everybody understands the challenge that the police and the security agencies have, and we all understand the capability gap they have with modern communications. This is going to be a step change for us, and that is why the discussions we are having with the Home Office are quite detailed, because we need to get this right. I am sure that everybody else on this panel, as well as me, wants to make this work and to ensure that taxpayers get good value for money. The only way we can do that is by having the strong discussions now, so we are very clear on what we need to provide and we do that in the most cost-effective way.

Mark Hughes: Regarding deliverability, without wishing to keep harping on about the same point, the easiest and most elegant way to deliver this capability is for over-the-top service providers to have the same obligations as companies here do today to assist law enforcement with information about customers who are using their services who may be breaking the law.

Q154 Lord Strasburger: On the subject of deliverability, Mr Hughes, you have twice said, "Then we will have to decrypt the data". How can you possibly do that unless you get co-operation from over-the-top providers, such as Facebook and others, or you get sufficient information from them as to how to decrypt that data, or from end users regarding how to decrypt their data? How can you do this?

Mark Hughes: You are absolutely right. The point of this is that we will have to be supplied with new technology, from law enforcement or intelligence agencies, to be able to decrypt that information about third parties and store it. That goes back to the point, again, that it is not preferable for our companies—certainly not for Vodafone—to be able to decrypt communications and store this. It would be much more elegant for the third-party service providers to have this obligation to assist law enforcement to fight crime.

Lord Strasburger: Presumably, by treaty, bearing in mind that most of them are American.

Mark Hughes: The Bill itself allows the Home Secretary to place an obligation on any person. Most, if not all, providers—certainly the big ones—have infrastructure and offices here. Given the way the internet is structured, there are things globally; I see no reason why the third parties would not want to assist with helping law enforcement in this space.

Stuart C McDonald: Mr Hughes, I think you said that you would not be able to attest to the accuracy of ICRs. Is that because of this process of decryption, or are there other reasons why you would not be able to do so?

Mark Hughes: It is fair to say that if we were able to extract data belonging to another provider, not understanding its structure as it crosses our network, I would be

uncomfortable with being able to explain the accuracy of another company's data. That would be an incredibly difficult thing for Vodafone to do.

Stuart C McDonald: So you might not be able to come up with accurate ICRs at all.

Mark Hughes: An ICR does not exist today. Once it is created and we have solved all the technical challenges that we have already discussed, I would imagine that it would be tested in court once this evidence becomes as bread-and-butter to the criminal justice system as mobile phone evidence is. I would imagine that it will be tested very heavily on the grounds of, "Who created it? How did you decrypt it? How accurate is it? If you did not create it, how can you attest to the accuracy of it?" Companies here, such as Vodafone, have to attend court to be cross-examined on mobile phone evidence that has been collected. We would find it extremely awkward to have to attest to the accuracy of data that we had not created in the first place.

Suella Fernandes: You appreciate, do you not, that the current lack in capability—for example, the requirement to keep internet connection records, or store them—means that the agencies can paint only a fragmented picture of a known suspect?

Mark Hughes: I absolutely recognise that.

Q155 **Suella Fernandes**: Examples abound, but in a recent referral of 6,000 profiles from the Child Exploitation and Online Protection command to the NCA, around 800 of those could not be progressed because of the lack of this capability. That is about 800 suspected paedophiles who were involved in the distribution of indecent images whose details cannot be gathered by the agencies. Bearing in mind the benefit that is gained by this storage and retention requirement, what alternatives do you think are viable while providing a similar benefit?

Jonathan Grayling: We are not necessarily questioning that there is an operational case for this. We work closely with the NCA; we work closely with CEOP. We are just trying to reflect the technical complexity involved in meeting the demands of law enforcement. We all have a duty of care as operators; we want to be good corporate citizens as well, but if the technical complexities are there, those are the facts, and we are trying to work through those with the Home Office to provide the provision that they are looking for.

The point that you raise there about CEOP goes back to the point about the knowledge of the law enforcement community. Certainly, the NCA are pretty advanced through the CEOP side of things in relation to trying to highlight these gaps in technology, and we work very closely with them on trying to close those gaps, but it is proving very, very difficult. The technology just does not exist at the moment.

Mark Hughes: I absolutely recognise what you are saying. We care passionately about assisting law enforcement. We take extremely seriously all the obligations that are placed upon us, and we do everything we can to give the best service to law enforcement through the system, with the things that we are obligated to do by law. As Mr Grayling has just said, we want to make sure that when this legislation passes and it has gone through the correct level of scrutiny, the obligations are technically workable and we can continue to provide the level of service that the police and law enforcement agencies expect from us. We get

how important this stuff is, and we really want to make sure that we can provide the data in the best way. Again, so much of this is going to be about over-the-top service providers that we must make sure it is achieved in the simplest way possible, and the simplest way possible is for those third parties to co-operate with law enforcement.

Suella Fernandes: In terms of maintaining the security of stored data, you use firewalls and personal vetting systems, and those are effective ways of keeping data secure.

Adrian Gorham: All the operators here are very experienced at looking after our customer data. We all have a layered approach; there are different systems and processes for keeping it secure. All this means is that we are going to have even more data that we will have to keep secure.

Interestingly, one of the parts of the Bill talks about a request filter, which will be run by a third party; a third party will take bulk data from us and analyse it for the police, to make sure the police only see the data they require. My concern there would be that that third party has exactly the same level of security that we deploy ourselves in our businesses. A number of us have international standards; I would expect that third party to have that level of security, if it has my customer data. I would expect the governance that we are putting in place to go and do audits on that third party, and I would—if I am giving them my customer data—expect to be able to go and audit them myself, to ensure that they are living up to our standards as well.

We are all very used to looking after security and protecting that data, but we now, with this Bill, have a third party whom we would need to give data to, and we need to be very sure that the same level of security is deployed there as well.

Q156 **Suella Fernandes**: Lastly, retention is subject to stringent controls; it needs to be necessary, proportionate, signed off by an independent person, and it needs to be compliant with various case law and the European Convention on Human Rights. What is your assessment of that consideration of lawfulness and effectiveness, combined with the exception of whether it is reasonably practical, as a sufficient safeguard to strike the right balance?

Adrian Gorham: The safeguards in the new legislation are very good. They are much improved on where we are now, and they are much more transparent. We have to ensure that the different auditing authorities do their roles and they are done properly. If you look at the recent audits they have just started doing on the operators with the ICO, they have agreed with industry what those audits will look like and what the definition and scope is going to be. The first actual audit was done last week on O2, so hopefully we will see the results of that come back. The one thing the Bill does very well is that it polices all the transparency in audit of what everybody is doing along that whole value chain.

Q157 **Victoria Atkins**: Mr Hughes, you have used the phrase "over-the-top providers" a lot. I may be the only person wondering this, but I suspect I am not: what do you mean by that?

Mark Hughes: The over-the-top providers I have referred to are companies that are running a communication service, such as WhatsApp, Snapchat, and Skype. They are examples of over-the-top service providers; they run a communications service using the underlying network providers that are here today.

Victoria Atkins: This is what I want to focus on. You have talked about how it would be more "elegant"—I think that was the word you used—for over-the-top providers to store this information, rather than you guys; sorry for being so informal. How on earth is law enforcement to know that one of the suspects that Ms Fernandes has referred to is on WhatsApp, Facebook or whatever unless they have that link in the middle, which is where you come in, signposting them to that application?

Mark Hughes: That is an excellent point. On signposting, we would have a role to play in saying, "We need to point you towards the company where you need to go to get the rest of the information about that customer", in a way they produce it and understand it. You make a good point about having to signpost the police in the first instance to what company has produced the communications service in question.

Victoria Atkins: If we just put that into the context of your evidence, you are not saying that your companies should play no role in this; you are worried about the details of decrypting and so on, but you understand that the Bill is phrased as it is to help law enforcement link a suspect to apps or services that they cannot know about unless you are involved in the middle.

Mark Hughes: Absolutely. This is about making sure that we do not blur the lines between traffic data and content by us having to open up all the packets of the data and then provide in an evidential way all the information to law enforcement.

Mr David Hanson: It is also about shifting the cost, is it not, from your perspective?

Mark Hughes: The Home Office has always had a policy of 100% cost recovery. They have assured us that this will continue. This is not an area that we make any money out of. We provide the very best service that we can to assist law enforcement.

Adrian Gorham: Another point worth making is that the customer of this is the police officer who wants the intelligence to allow him to make that arrest. If he believes that his target is using Facebook, the target may be using Facebook but it can use it on many different bearers. So it may use the O2 network; it can then go into a Costa Coffee and use a wi-fi network; it may then go somewhere else and use BT's wi-fi. It can use many different bearers, and you have to somehow get all that data from those different companies and put that all back together to show what that individual was doing on Facebook. If you go to Facebook and they have the encryption keys, they can tell you what is going on. They have all that data for that individual, so I do believe that it gives a much better service to the police to go to that one point of contact than try to go to each of the bearers that are carrying those communications.

Q158 Stuart C McDonald: You referred earlier to the process of setting up filter arrangements to get that communications data. What is your understanding about how request filters will work under this legislation, and would you have any concerns about the operation of request filters?

Simon Miller: We understand that the request filter is a mechanism by which large amounts of bulk or collateral data provided by us as communications service providers, as a consequence of requests made by law enforcement agencies, will be gradually—through a process of correlation and different data points—narrowed down to identify either a single

subscriber or a smaller subset of users, and that this will be done by a trusted third party. The whole purpose of this request filter is to minimise the amount of unnecessary bulk data that will be handed over to law enforcement agencies.

We are all agreed as to the principle of this. There are a number of concerns, which Mr Gorham has alluded to, regarding the detail. The first is the fact that we would still continue to provide bulk data to a third party, and in so doing could be in breach of our duty of care under the Data Protection Act and the Privacy and Electronic Communications Regulations to our customers' data. The second is that we have absolutely no detail on what this trusted third party would look like, the form it would take, or the legal obligations that it would be under. As a minimum, we would simply expect that whatever operation the request filter undertook was done to the same standards, and was as secure, as our own arrangements.

Stuart C McDonald: So you have no idea who these third parties would be at all.

Simon Miller: Not yet, no.

Stuart C McDonald: What exactly is the filter? Who is responsible for putting that together, and would you have any ability to review what the filter was doing to your data?

Mark Hughes: I do not know who would be providing the service. I think it would be for the Home Office to select a vendor, to be able to build that situation. In principle, it is a good idea to be able to prevent lots of collateral intrusion. When you have really big, complex inquiries that you are running as a police officer, where you may need lots of data, the filter can be a way of reducing the collateral intrusion. The important thing here, as Mr Miller just said, is that whoever operates that has to operate it to the same standard in terms of the data that is being provided out of it, because this could fundamentally change the way network operators give evidence in court. Remember: we are potentially providing information into the filter. The operation, and what changes in the middle and what ends up on a police officer's desk from the query they have run is being provided by a person in the middle, a third party service—a vendor in this scenario. Again, we would need to make sure. It is going to take a lot of close collaboration to make sure this works well.

Stuart C McDonald: What sort of things would you want to see in the Bill so that you could have faith in that filtering process by the time you arrive in court to speak for the accuracy of the data you have provided?

Mark Hughes: We want direction and understanding on which parts of the evidential chain we would be expected to stand up in court and be cross-examined on, and whether, if the data had changed in the middle in some way, it would be the third party—for example, in this case, the vendor who is providing the service—that needed to attend court. I appreciate that these are sort of in the weeds, and they are quite technical things that we need to be thinking about, but essentially we are giving evidence in court on a day-to-day basis on mobile phone evidence, and we are worried about making sure that we can continue to do that with what is essentially a new piece of kit in the middle of the network.

Simon Miller: At the moment, this may be an issue for guidance, but these are discussions that the Home Office is yet to have with us, so we are dealing with an unknown. We are very keen that these discussions continue, and that these issues are bottomed out.

Stuart C McDonald: Any further thoughts?

Jonathan Grayling: Just to reiterate, the panel has said that the Bill places an obligation to provide security controls in relation to retained data, and those security controls are audited and will be audited. What is not in the Bill is that there are similar security controls for the request filter, and subsequently the customer data—my customer data that I am supplying to the filter. I would like to see the filter having the same security controls as the ones CSPs are compelled to provide in relation to retained data.

Q159 Matt Warman: Can you say a bit about what you understand by a technical capability notice, and what you understand by the Home Secretary being able to impose one at will?

Mark Hughes: Our understanding is that this is about the potential for equipment interference. Vodafone has three real concerns about this particular item. First, equipment interference could obligate a network operator to introduce, say, a backdoor or a way to launch some kind of attack against a particular target that may be using the network. You will probably not be surprised to hear that we have three concerns. First, we are worried about this representing a real diminution in trust in UK-based service providers, which may have to introduce backdoors on their network. In such a highly competitive marketplace, if you had to decide who to place your communication service providers with—a UK-based company that potentially has this obligation, or somebody else who does not—you may be really thinking about that.

Secondly, we are concerned about an obligation that may ask us to fundamentally reduce the level of security of our products or services, or our networks. We would be really concerned about introducing any reduction in the level of security of our products and services. Thirdly, we understand that, as it is written in the Bill, this may involve our people and our staff having to get involved in launching such attacks against targets across our network. We would be keen to make sure that that does not happen, and it is down to the law enforcement or the agencies to manage the workable provisions of that.

Matt Warman: Any other thoughts?

Jonathan Grayling: I would echo what Vodafone said there. With respect to the Bill itself, there are a number of aspects of control and oversight over those technical capability notices that we do welcome—significantly, the fact that the Home Secretary has an obligation to consult with the respective CSP prior to serving a technical capability notice on that CSP. That consultation has to take into account, among other things, proportionality, technical feasibility, the cost—which is significant for us—and the impact on our customers and our network.

Even after that consultation process, and a notice is served, there is still a mechanism whereby if the CSP is still unhappy or concerned with that notice, they can pass it back to the Home Secretary for further review and, again, the Home Secretary has an obligation then to consult with the Technical Advisory Board and the IPC, which we welcome. The key point here is that we need to ensure that each stage of that process is rigorously enforced, rather than a rubber-stamping process. If we have concerns about that, we want to have it demonstrated that the appropriate oversight and controls are being applied to that process.

Just one very quick, final point. My understanding of the Bill is that the IPC would have responsibility for the oversight of national security notices. I cannot find anything in the Bill that says that the IPC would have oversight for technical capability notices, so the question is why that might be the case.

Matt Warman: What do you think your customers would make of even an oversight arrangement that you were corporately happy with?

Jonathan Grayling: Customer trust is essential to our business, and the priority for us is to ensure that we provide a secure and resilient network. That is what our customers will expect. If there are any powers or any activity that is undertaken by the agencies in relation to equipment interference, whether that is proportionate and lawful is a matter for Parliament and the agency itself, but EE would not accept it if those activities had any impact on the security of our customers' data or the resiliency of our networks.

Q160 **Matt Warman**: Moving on to the IPC that you mentioned, do you think that the level of engagement that is outlined in the Bill between you and the IPC is sufficient to maintain that level of security and trust?

Simon Miller: The levels of engagement envisaged are broadly similar to those that we have currently with existing authorities. Interject, gentlemen, if I am talking out of turn, but those levels are appropriate to the subjects concerned. The issue for us has always been that they are broadly uncoordinated, and as a consequence of that there are business impacts. In particular, at the margins, there are jurisdictional overlaps with different authorities talking to the same subject with different voices. It therefore follows that we are fully in favour of the creation of a single body, the IPC, that will have all these powers of oversight, and it will rest in that one body. The simple fact of the matter is that the current practice of having separate bodies with these different functions is, for us, broadly cumbersome, open to misinterpretation and misunderstanding, and time-consuming.

As for the actual level of engagement, this would be a new body. We would fully expect levels of engagement to ramp up as that body beds in and to have to adapt to new personnel and new ways of working. It is probably worth saying at this point that the relationship that we all have with IOCCO is an exemplar. If the IPC were to look at the ways of working exhibited by the existing authorities, it should look to IOCCO as a model of best practice, and we would very much like to see those practices demonstrated around building strong, coherent stakeholder relations, early engagement and demonstrating sector expertise continue.

Matt Warman: Broadly, it sounds as though you are looking forward to the changes that are coming, rather than dreading them.

Simon Miller: Absolutely.

Adrian Gorham: It might also be useful if there is an express right for the operators whereby if we have an issue or a complaint about one of the LEAs or the police we can go directly to the IPC to report that. That is not to say that there have been any issues previously with them, but it is worth having in the legislation so that we have that channel should we want to use it in the future.

Q161 **Lord Strasburger**: Would you agree that equipment interference is one of the most technically complex and risky activities that we are looking at in this Bill, and do you think there is a case for having some sort of technical oversight as to what you are being asked to do from a third party, as well as having judicial oversight?

Jonathan Grayling: In the Bill, there is a mechanism to refer to the Technical Advisory Board, and we would expect that Technical Advisory Board to provide that independent oversight. Because of the additional obligations in the Bill, there should be a review of the TAB to ensure that it is structured appropriately and has the appropriate individuals around the table with the appropriate knowledge. That is necessary.

Lord Strasburger: These are very specific skills, are they not?

Jonathan Grayling: They are.

The Chairman: Thank you very much indeed. We have now come to the end of the formal session.

Professor Sir David Omand GCB, Visiting Professor, Department of War Studies, King's College London (QQ 76-93)

Evidence heard in public Questions 76-93

Oral Evidence

Taken before the Joint Committee

on Monday 7 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Bishop of Chester, Lord Henley, Lord Strasburger.

Witness: **Professor Sir David Omand GCB**, Visiting Professor, Department of War Studies, King's College London, gave evidence.

Q76 The Chairman: We extend a very warm welcome to our four guests this afternoon. We are very grateful to all of you for coming along on what is a hugely significant Bill that is going through Parliament—the Prime Minister called it the most important of this Session. Thank you very much indeed. As you probably know, the procedure is that I will kick off with a question or two, and then my colleagues will in turn ask you various questions on different aspects of the Bill that I think you find very interesting. If, when I ask a question of an individual, he wants to preface his remarks with a short statement, that is entirely up to him. I turn first to Dr Bernal. After you have answered, colleagues will be able to come in. What are your views on the draft Bill? Does it deliver the transparency on investigatory powers that you have particularly called for?

Dr Paul Bernal: Perhaps the best way to put it is that it goes part of the way. As far as I am concerned, it is good to see everything in one place, or almost everything—some bits are clearly missing—but for proper transparency we do not need just the Bill; we need the process to work properly as well. I would have said in my introductory remarks, had I made any, that the timetable makes it very difficult to get as much scrutiny as we would like; we have been called here very rapidly, and you have only a few weeks to do this. For transparency to work properly we have to have the chance and time to put our analysis into action. It is a bit difficult to do that.

One other thing I would say about transparency is that certain terms are used and expressed in a way that is not as clear as it could be. There are terms like "bulk powers" when we do not really know how bulky "bulk" is, if you see what I mean. For things like Internet connection records, it has taken some time, and we are still only part of the way there, to tease out what it really means. From that perspective, it is good to have it all in one place, but the process needs to be stronger. We need to make sure there is enough time to do it, and I am not sure you have as much of it in this Committee as you would like—perhaps later on there will be time—and we have to tease out some of the terms more accurately.

There is one other aspect. Some of the things in the Bill will become dependent on codes of practice and similar things that go with it. For transparency's sake, so that we understand what is going on, those codes of practice need to be put in a form that we can all see prior to the final passage of the Bill.

Q77 The Chairman: You have touched on the second question I was going to ask, so I will raise it now. You mentioned the codes of practice, which are hugely important in all this. What do you think the legal status of those codes might be?

Dr Paul Bernal: The legal status of the codes depends a little on how the final Bill turns out. From our perspective as legal academics, the key thing about codes of practice is not so much their legal status, which, depending on how it is set out, will be clear, but the extent to which they are also subject to the level of scrutiny and attention that the Bill itself is. It is easier to pass a code of practice through a small statutory instrument than to pass a whole Bill with full-scale scrutiny. We want to make sure that the codes of practice, which can be the critical part, get the same degree of scrutiny and attention both from people like us and from people like you.

The Chairman: With regard to the timetable, of course the issue that affects both this Committee and Parliament is, as you know, the sunset clause in the current legislation. Parliament has now laid down the amount of time we have. We certainly ensured that we gave ourselves extra and longer sessions, including in and around Christmas, and I am quite convinced that both Houses of Parliament will give it very thorough investigation, as indeed they should, but the point has been made. Does anybody else wish to speak on those issues?

Professor Sir David Omand: If I may make two remarks, the first is to stress the importance, in my opinion, of the Bill as the culmination of 500 years of history. It has taken 500 years to put the secret surveillance activities of the state under the rule of law. For centuries we had the royal prerogative being used in secret. Parliament passed the device of the secret vote but asked no questions. We had executive regulation in the last century, and for the past couple of decades we have had a patchwork of provisions in legislation, so all that secret activity was lawful but not understood. This Bill now places it under the rule of law; it will be comprehensible to the citizen. I cannot overestimate the importance of the Bill.

The second point is to agree strongly that it is in the codes of practice that the public will find it easiest to understand what is going on, rather than in the technicality of the Bill itself, so the codes are very important. Schedule 6 to the Bill sets out very clearly what the status of those codes will be. They will have to be presented to Parliament, along with the enabling statutory instrument.

The Chairman: Professor Anderson or Professor Ryan, are there any comments you would like to make at this stage before we move to other questions?

Professor Ross Anderson: I believe you will be asking me in due course about Internet connection records.

The Chairman: We will.

Professor Ross Anderson: It would be great if, in addition to having codes of practice, we had very much greater clarity on definitions. I will discuss Internet connection records, but there are other things that are not really defined at all, from the great concept of national security down to some rather technical things. I hope that clarification comes out during the Bill's passage.

The Chairman: You think such definitions should be on the face of the Bill.

Professor Ross Anderson: Yes.

The Chairman: Professor Ryan, are there any initial comments you would like to make to the Committee?

Professor Mark Ryan: Just on questions 1 and 2?

The Chairman: At this stage, yes, because there will be other more detailed questions, some of which will probably be directed to you personally as well, but at the beginning of the session would you like to make any general comments?

Professor Mark Ryan: The comment I would like to make about transparency is that this seems to be such an important area that the kind of oversight proposed is not enough. One would need more quantification of the sort of surveillance that takes place. Of course, I am aware that surveillance has to be done in secret, but I believe that the quantities of surveillance and the nature of surveillance can be disclosed to people without compromising the secrets of the surveillance activity. That seems to go more towards transparency and is much stronger than mere oversight, so I believe there should be more of that.

Q78 **Dr Andrew Murrison:** You have covered a huge amount of ground in about seven minutes. You hit the nail on the head in terms of definitions and the need to ensure that codes of practice and statutory instruments are sufficiently transparent and that scrutiny is of the utmost. I am interested to know how you think scrutiny and transparency can be improved other than through the normal process of laying statutory instruments before the House, because I sense from what you said that you feel that the Bill, which talks about SIs and codes of practice, is not sufficient in that respect.

Dr Paul Bernal: I would not say exactly that it is not sufficient. What I am interested in is getting as much scrutiny as we can. In order that we can understand the Bill we need to have the codes of practice at the same time, at least in draft form, so that they can be examined; frankly, to understand some of the powers in the Bill without a code of practice is very difficult, particularly on things like bulk powers and Internet connection records. We will talk a lot about Internet connection records later, but they are defined in such a way that it is unclear on the face of the Bill exactly what they will mean in practice.

Historically, not as much attention is paid to statutory instruments by the House. You do not spend as much time passing them as you do Bills; you do not have Committees scrutinising each of the statutory instruments at the same level of detail.

Dr Andrew Murrison: But it is worse than that, is it not? This is a very rapidly moving field, so you cannot reasonably lay all the codes of practice and anticipate all the SIs at this time, since 12 months down the line there may be yet more to come.

Dr Paul Bernal: Yes, and that is a fundamental problem with any kind of Bill in this area. I do not know whether there would be a mechanism to produce better scrutiny of the codes of practice, but attention should be drawn to the fact that this will be important as it continues. It needs constant attention, not just at the moment we pass the Bill.

The problem with the Regulation of Investigatory Powers Act was that, although it got a lot of attention at the time, the things that gradually built up to create the confusion—chaos is not quite fair—for people about the overall regime, and which stimulated the need for this Bill, were not sufficiently attended to over the years as things happened. We need to make sure that does not happen this time around.

Dr Andrew Murrison: Do you think a sunset clause would help? We are replacing one sunset clause with another. Is that inevitably where we are going to be led?

Dr Paul Bernal: Frankly, in this area you need sunset clauses in almost everything, because the technology moves and the behaviour of people changes. The overall situation changes. You need to be able to review these things on a regular basis, and a sunset clause is one of the best ways to ensure that happens.

Professor Ross Anderson: Last time around how we dealt with this was that, in the run-up to the passage of the Regulation of Investigatory Powers Bill through Parliament, a number of NGOs organised a series of conferences called Scrambling for Safety, and afterwards various statutory instruments were laid before the House. We are proposing to do the same again. The first Scrambling for Safety workshop is to be held at King's College London on 7 January from 1 pm to 5 pm, and all members are of course very cordially invited. We anticipate that it will be the first of a series that will enable engineers, lawyers, policymakers and others to dig into the meat of what is going on, exchange views and push the thing forward.

Q79 Suella Fernandes: Based on your expertise, would you set out briefly the nature and extent of the problem or threat we are facing when it comes to the use of this technology?

Professor Ross Anderson: The problem with the use of surveillance technology is that, if it is used in ways that do not have public support, it undermines the relationship of trust between citizens and the police, which has been the basis of policing in Britain for many years. Sudden revelations like Snowden are extraordinarily damaging because they show that the Government have been up to no good. Even though the Government may come up with complicated arguments about why bulk equipment interference was all right under Section 5 of ISA and so on, it is not the way to do things. There was a hearing in the Investigatory Powers Tribunal last week on that very issue.

There are other issues. The first is national leadership. If we go down the same route as China, Russia, Kazakhstan and Turkmenistan, rather than the route countries such as America and Germany have gone down, there is a risk that waverers, such as Brazil and India, will be tempted to follow in our wake. That could lead to a fragmented IInternet, with

extraordinarily severe damage for jobs, prosperity, international stability and, ultimately, the capability of GCHQ to do its mission, because if you end up with the IInternet being partitioned into a number of walled gardens, like the Chinese or Iranian ones, they will be very much less accessible to the intelligence agencies.

In addition, if the powers are abused, or seen as capable of being abused, there could be exceptionally serious damage to British industry. If people overseas come to the conclusion that, if they buy a security product from a British firm, it may have a GCHQ-mandated back door, they will not buy it; they will buy from a German firm instead. This is where the rubber hits the road when it comes to overreach in demanding surveillance powers.

Professor Sir David Omand: On the other hand, my advice to the Committee would be that this Bill contains the basis of the gold standard for Europe. This is how you get both security and privacy in respect of freedom of speech. The interplay of checks and balances and oversight regimes means that none of what Professor Anderson has described needs to happen. Of course, with a malign Government and agencies that flouted the law it would be possible to have abuses. I do not believe that either is likely, and certainly the provisions in the Bill allow this House to maintain very strict control of the Executive in its use of these powers.

Professor Ross Anderson: With the greatest respect, the reaction of America and Britain to the Snowden revelations has been somewhat different. In America people have rowed back in all branches of government. For example, President Obama has, simply by executive order, commanded the NSA to minimise the personal information of unaffected foreign nationals, like us. The legal branch has seen to it that, for example, national security letters, which used to be secret for ever, are now disclosed after three years, and Congress failed to renew provisions for the retention of American citizens' communications data. All branches of government have pushed back and sent a solid signal to the world that America cares about privacy and the proper regulation of its law enforcement and intelligence services. If the reaction from Britain is different, even if powers are not abused, it still sends a signal to the Brazils, Indias and, may I say it, the Kazakhstans. We do not really want that.

Q80 **Bishop of Chester:** A sunset clause is the nuclear option of legislation, but reading the Bill I am wondering how there is a process of inbuilt review, because the scene is changing so fast. There is a technical supervisory board bringing together stakeholders and so forth. Should there be an inbuilt power to renew the provision? That has been in some previous terrorist legislation. There has not been a formal sunset clause, but there has been a renewal motion. That would force Parliament to review what is happening, because for the legislation to continue there would have to be a renewal notice.

Professor Sir David Omand: Of course, it is Parliament's prerogative to put in such a provision. My experience in the public sector is that it should be done very sparingly, because it may turn out that at precisely the moment you have to legislate afresh, as with DRIPA, Parliament may not actually want to legislate afresh. One concern I had was whether the definitions in the Bill were sufficiently robust to deal with technical change. Having studied them, I am as confident as I can be that they avoid hostages to fortune, so your House will not discover in a couple of years' time that a different Bill is needed because the technology has moved on, but that will need to be examined by detailed scrutiny.

Q81 Shabana Mahmood: My first question is to Professor Anderson and then his colleagues. We have two competing narratives of the Bill: one that these are significant new powers and major changes, and the other that it is just codifying current provisions and bringing them more obviously and explicitly within the rule of law, as Sir David suggested. Professor Anderson, what is your view as to which of those narratives is more accurate?

Professor Ross Anderson: The Bill has been marketed as bringing in only one new power, namely Internet connection records, but it does many other things as well. For example, when the Regulation of Investigatory Powers Bill passed through this House and became an Act, one of the things we lobbied for and secured was the provision that if the agencies wished to command somebody to decrypt something, or hand over a cryptographic key, there should be special safeguards. The City of London did not want a rogue superintendent, perhaps in the pay of a criminal gang, to approach a 24 year-old assistant shift supervisor at a bank's data centre somewhere in east London and command him to hand over the bank's master signing key. Therefore, the provision was made that the production of a cryptographic key had to be demanded by a Chief Constable in writing and the letter had to be presented to a main board director of the bank. There are many provisions like that which appear to be swept away by this new legislation. Parliament must realise that the arguments are just as strong today as they were then; otherwise, how are you going to persuade international banks that London is a good place to do business? Some banks already had issues last time around.

My second comment is that a number of things that were previously done secretly were made public only in the run-up to this Bill, which enables the Bill team to say, "This is old stuff. We knew about it already". I refer members to the Investigatory Powers Tribunal hearing and the long arguments therein about whether an ISA Section 5 warrant could be used for bulk interception or only targeted interception. There are many technical aspects like that.

Thirdly, although the Internet connection record is ostensibly the new thing in the Bill, it actually gives very much greater powers than have been advertised; rather than just helping IP address resolution, it enables a policeman to say, for example, "We have these two bad people. Show us all the websites they both visited last month, and tell us the names and addresses of everybody else in the world who visited the same addresses". That is an extraordinarily powerful capability. It is the sort of thing that Internet service companies use to fight spammers, phishermen, click fraudsters and so on. Those of us who have worked in that field know how powerful it is and tend to be of the view that it should be classified along with intercept. If we are to have a special higher burden for intercept warrants, that higher burden should apply also to complex queries that are made on traffic data.

Shabana Mahmood: Have you done any analysis of powers advertised one way but which, as you suggest, lead to, say, five extra things? Have you made some sort of qualitative analysis to back up the examples you are helpfully giving us?

Professor Ross Anderson: The qualitative analysis basically comes from experience working at Google on sabbatical four years ago with the click fraud team. Knowing that such inquiries are extremely powerful, and talking to colleagues at Yahoo and Facebook recently, there is general concern that, if you allow people to make complex queries like that, it is up

at the level of a box of fancy tricks; it is not the sort of stuff you want to let an ordinary policeman do without supervision, because it can be used to do some very bad things.

Professor Sir David Omand: The Bill does not provide for ordinary policemen just to request that. There is a mechanism for a single point of contact and independent agreement before data can be acquired. I do not recognise either of the extreme cases Professor Anderson puts forward, but no doubt the Committee will need to investigate that further.

Dr Paul Bernal: If I may add something in response to that, there is something missing in the idea that these are either new powers or old powers. People's behaviour has changed fundamentally. The Internet, which was a medium used for communications—in the old-style idea of communications—is now used for almost everything else: shopping, dating, research and that kind of thing. The same power applied in a different situation gives a significantly higher level of intrusion than we have ever seen before. It is not like listening to phone calls, reading emails or things like that; it is like following people down the street while they shop, looking at the books they take out of the library and things like that. Without even changing the law, you are significantly changing and increasing the level of intrusion. It has lots of different implications, not just in terms of the balance of privacy and things like that but all the other rights we normally think of. Our expectations of privacy are different from those we had in the past. In a way, it comes down to the idea of how the law is going to change and how we need to take things into account. We need to take into account not only developments in technology but the way people's behaviour changes in relation to that technology; for me, in effect, that is the biggest increase in power. It is not that there is a new power built into the Bill, but because we use communications so much more extensively it is a much more intrusive thing to do any kind of Internet surveillance.

Professor Sir David Omand: That is why the Bill defines event data, Clause 193, in a conservative way, not taking modern metadata but imposing on the rather fuzzy reality some precise definitions, to minimise—it cannot be avoided completely—the kind of case Dr Bernal referred to. Inevitably, if you impose strict definitions on fuzzy reality, you will occasionally get hard cases. Those will exist in this world. As we know, the difference between dangerous driving and driving without due care and attention means that sometimes cases fall on the wrong side of the line, but the old adage that you do not make law by hard cases still applies. I commend to the Committee the way that the Bill has not expanded the definitions of communication data in defining event data.

Q82 Shabana Mahmood: That is helpful. You touched briefly in your previous answers on my final question, which is about future-proofing the Bill to take account of the pace of behavioural and technological change. We had evidence from officials from the OSCT. They were very bullish and confident that the changes in relation to Internet connection records in particular meant that it was sufficiently future-proofed. Could we have your comments on that?

Professor Ross Anderson: I have two main comments. The first is from the viewpoint of the long term—20 years out. We are simply asking the wrong question. The right question is: what does the police service look like in a modern technological society? Is it completely centralised? Does it go like Google? Do Ministers take the view that a chap sitting in Cheltenham can learn more about citizens in Leicester than a bobby on the beat in

Leicester? What sort of society does that become? This is a much broader conversation than just about who gets access to whose mobile phone location trace when.

The medium-term issue, which I think will become acute over a period of five to 10 years, is that the real problem is a diplomatic one. The real problem is about jurisdiction and how we get access to information in other countries, specifically America. America is where the world's data are kept. If they are kept in Finland or wherever because of cheap electricity, usually they are still controlled by a US company. There are some exceptions—Korea, Japan et cetera—but this is largely about how we get access to American data.

That means, like it or not—and many people are beginning to come to this conclusion—that the real fix for this is a cyber-evidence convention, like the cybercrime convention. That will involve diplomatic heavy lifting and an agreement, perhaps initially between America and the European Union, with other willing countries joining later as they wish, that provides a very much faster service for getting at stuff than the current mutual legal assistance treaties. For that to work, there are three things we almost certainly have to have. The first is warrants signed by judges, because that is what America expects. The second is transparency, which means that if somebody gets wiretapped you eventually tell them—when they get charged or after three years or whatever. The third is jurisdiction, because the real bugbear for companies like Google at the moment is that a family court in India gives it a warrant saying, "Please give us the Gmail of this person in Canada", who has never been to India. How do you simultaneously employ engineers in India and give privacy assurances to your users in Canada? That is why at present all this stuff gets referred to lawyers in Mountain View. That is the real problem, and it is time the Government faced up to it.

The Chairman: Professor Ryan, do you want to say something regarding an earlier point?

Professor Mark Ryan: I want to go back to the question of whether these are new powers or existing ones. Following what Dr Bernal said, one of the very huge powers that exists in the Bill is bulk equipment interference—that the state can interfere with people's computers on a bulk scale—which means that people who are not guilty of any crime, nor even suspected of any crime, may have malware put on their computers by intelligence services to collect vast amounts of data on innocent people in a kind of funnel, so that eventually criminals can be caught, but the people who are being subjected to that are not criminal at all. That seems to me to be an extremely dangerous thing in a free society. I do not think that the kind of oversight proposed in the Bill goes anywhere near being able to control that type of activity.

Professor Sir David Omand: The bulk equipment interference warrant can be sought only by the intelligence agencies in order to acquire intelligence relating to individuals outside the UK for the purpose of national security. For the sake of clarity, the Bill already restricts that.

Q83 Lord Strasburger: Sir David, your career was spent in senior positions in the Civil Service deep inside the security establishment, which probably makes you, of the panel, specially qualified to answer my question. It seems that over the past 15 years decisions were made behind closed doors to introduce several of the most intrusive and least overseen powers in this Bill without bothering to seek Parliament's approval. Why was it considered acceptable in

a democracy to bypass Parliament and introduce large-scale and highly controversial surveillance powers without Parliament's explicit approval?

Professor Sir David Omand: I can only hazard an answer, which is that the legal regime under which previous Governments operated for the past 20 years, since the 1980s, was what I would describe as legal compliance; in other words, if it could be done lawfully under existing powers that Parliament had passed, Ministers would authorise such activity, after due legal advice, regardless of party—this is not a party political matter—in the interests of national security, the prevention and detection of serious crime, and economic well-being arising from causes outside the United Kingdom. That was the regime.

It was really when the Investigatory Powers Tribunal took the case and reported that the Government's activity, in particular GCHQ, might be regarded as lawful under the individual statutes but failed the rule of law test because it was not clear, as your question implies, to the public—

Lord Strasburger: Or to Parliament.

Professor Sir David Omand: Or to Parliament. This Government have taken that to heart, and the Bill is in part the result. We have moved into a new era and I am personally very glad of that. A lot of trouble would have been saved if, say, even five years ago the codes of practice—it would not necessarily have taken new legislation—on equipment interference, investigative powers and so on had all been updated to the modern digital world. For one reason or another that was not done. The shock of discovering what was happening, for very good reason—to defend the public and our security—was all the greater. I think the lesson has been learnt.

Q84 **Victoria Atkins:** I have a question for Professor Anderson and Dr Bernal. You talked a lot about privacy and, in particular, the debate in America about privacy. One thing that strikes me about the whole discussion is that very often we are focusing, if I may say so, on the worst-case scenario as to what the intelligence services and the Government will do with people's information. What are your views in relation to the computer companies that hold all this data about us? If we google a dating agency, Google will have that information. What are your views on those bodies, because to me they are very much part of the debate about privacy?

Professor Ross Anderson: Yes. I tend to take different views of different companies because of their different internal cultures. Having worked at Google, I understand and to some extent trust the culture there.

Victoria Atkins: You worked at Google.

Professor Ross Anderson: Yes, four years ago on sabbatical, so I understand it. My colleagues have worked for other companies. Fundamentally, whether you are a company that tries to be good or a company that is a bit less scrupulous, the underlying fact is that the modern economy depends on people trusting large service companies with their data, because it is so much more efficient to have 100 million people's data in a data centre than it is for everybody to be backing up their own hard drive at home and losing their photos

and everything. That trust has to be maintained. If it is lost, the consequences could be dire for economic growth and the companies concerned.

People talk about worst-case privacy scenarios, but that is how people talk; that is how the media and politics operate—they operate by stories. The human brain is optimised for stories; it is how people remember stuff. If you get the perception out there that in the UK people who offer services have to leave a government back door, or remove the encryption if ordered, or whatever, it could be extraordinarily damaging for British business.

Victoria Atkins: Does selling people's data come into that? Are you comfortable with Google's position on that, having worked for it?

Professor Ross Anderson: Personally, I do not click on ads. If you want to go to a company that does not sell data, you can go to Apple or you can go to the trouble of having everything private. For example, I take the view that, if I am sending an email that I do not mind the FBI reading, I use Gmail; if I am sending an email that I do mind the FBI reading, I use something else. That is also the conclusion to which I think more and more users generally, and young people in particular, are coming to.

Q85 **Matt Warman:** I have a question for Dr Bernal primarily. As an example of new powers in this Bill, you said it was like following someone down the street and seeing which shops they go into. It strikes me that we have long had the power under certain circumstances for people to be placed under surveillance and followed down the street to see which shops they might go into. Could you give the Committee an example perhaps when we get back?

The Chairman: Order. There is a Division in the Commons, so we will adjourn for 10 minutes. I am sorry about that.

The Committee suspended for a Division in the House of Commons.

Matt Warman: To recap briefly, you cited the example of following a person down the digital street under authorised surveillance, which strikes me as a digital updating of analogue powers we have already. Could you offer the Committee an example that is not simply a digital updating of existing analogue powers and is genuinely novel because it is digital?

Dr Paul Bernal: It is a very important question, and there are lots of issues related to it. There are some things that we do in the real world, or the offline world, that we feel comfortable being observed doing. We have CCTV cameras in the streets, we have them in shops, and so on. We do not have them in our bedrooms, we do not have them staring at our diaries all the time and we do not have them monitoring exactly where we walk. We get the choice: do we want to go to this place where we know there is CCTV, or that place where we know there is not CCTV? That is one of the important differences.

The thing about the Internet as it is now, particularly for younger people, is that they do literally everything on it; there is no aspect of their lives that does not have an online element. If you have a system as is proposed with Internet connection records, for example, where there is some gathering of their entire browsing habit, not beyond a certain level—I hope we will get on to Internet connection records later—at least you have knowledge

about what they are doing in every aspect of their lives. When you go to the doctor, you expect confidentiality from your relationship with the doctor when you discuss your health issues. If you visit a website to research a particular health condition, that may reveal just as much about you as you would reveal to your doctor—in fact, many times more than you might reveal, because people have a sense that they can get more intimacy by doing things on the Internet than they might even be prepared to admit to a doctor.

There is another element. We talked a little about Google and others. Given the way profiling works for almost all commercial Internet companies, and the way big data analysis works, you can draw inferences from relatively small amounts of browsing data that can then be used to infer stuff that you would otherwise keep private. An example is your sexuality. You might not want to reveal your sexuality, but big data can make a probable analysis of it with a relatively small number of places you visit on the Internet.

It goes back to the question about whether we are looking at extreme cases. We are looking at extreme cases in some ways, but we are also looking at very ordinary cases. What we all do on the Internet has an impact on credit ratings, insurance premiums and things like that. They can be based on very basic information that can be gathered about how we behave.

I am sure David will say that safeguards are built into the Bill so that it can be used to do only certain things, but that is not really the whole story for two reasons. One is that data, wherever they are and in whatever form, are vulnerable in many different ways. The example that comes most readily to mind, because it is so recent, is TalkTalk having been hacked, and holding exactly the kinds of records that we are talking about. That information is ideal for ID theft, credit card fraud, scamming and things like that.

If we gather those Internet connection records, we are basically creating a very targeted database, which says on the front, "Hack me, please, if you want to get ideal information for these kinds of crimes". We need to be careful not just about what we think the Government are going to do. Like David, I trust to a great extent our security services and police, but we are creating something that can be misused by other people, not just by them. There are many ways in which that can happen.

Q86 Suella Fernandes: In terms of legality, the issuing of warrants is subject to the test of it being necessary and proportionate. In light of that, what is your view on its compatibility with proportionality as required under the ECHR?

Professor Sir David Omand: Proportionality and necessity are in the Bill. They are written in, as they are in the current legislation. Dr Bernal's examples were very good ones of why digital mass surveillance is a thoroughly bad idea. Thankfully, it does not happen now, and under the provisions of this Bill it could not happen in the future either. The question that I suggest the Committee really needs to address is how proportionality is assessed—precisely your question—not just in relation to the granting of a warrant but the whole process through which the selection of material for examination by human beings—the analysts—takes place. The IPT, the independent court, has examined this; senior judges who oversee interception have examined it, and they are satisfied that the current procedures are consistent with the Human Rights Act, Article 8 and thus respect privacy. Equally, there is no reason why the provisions cannot be applied in practice in ways that remain consistent.

The decision on proportionality and necessity rests with the person signing the warrant. The Home Secretary has made her view clear in the Bill. I am disappointed that she decided that she had to sign police warrants and that they would not go direct just to the senior judge for approval, which was our recommendation in the independent review commissioned by the former Deputy Prime Minister, and that would be more consistent with David Anderson's review. I strongly believe that the Home Secretary or the Foreign Secretary, as appropriate, should sign the warrants relating to national security and the work of the national intelligence agencies, for which they are statutorily responsible to this House. The police service is in a different constitutional position, and I would have thought that purely police matters could go straight to the judge. It is no harm that the Home Secretary signs as well; it is just additional work.

Dr Paul Bernal: Can I go back to the question of proportionality? One of the key things is not just about the warrant to access the information. One of the key elements of proportionality is the gathering and holding of the information itself. The CJEU has consistently—even more so recently—held that the holding and gathering of the data engages Article 8, and that indiscriminate generalised holding and gathering of data is contrary to fundamental rights. That was held in Digital Rights Ireland; in the Schrems case it was part of the key reason why the safe harbour decision was invalidated. This is not because they have some perverse view that does not match with reality but that the European Court has started to understand the impact of holding all this personal data. It is not just the warrants—to a degree, I agree with David about the warranting process; it is the gathering of the data that I disagree with, particularly the way Internet connection records are set out. All this data seems to me to be gathered on the assumption that that is all okay and it is just the accessing we need to deal with. I cannot see how this law would survive a challenge in the CJEU on that basis.

Professor Sir David Omand: I very strongly disagree. I am not a lawyer, but it seems very clear to me that the Schrems and the Digital Rights Ireland judgments do not bear on the point that has just been made. Those judgments did not consider the question of proportionality of collection and selection, which is not indiscriminate collection of data willy-nilly. You might want to take advice on that.

Professor Mark Ryan: I want to comment on the bulk provisions of the Bill, because they allow for the collection and automatic processing of data about people who are not suspected of any crime. Therefore, I do not think it is correct to say that this is not a recipe for mass surveillance. It is the processing of data about everybody, and in my opinion that is mass surveillance.

Professor Sir David Omand: But it is not processing data about everybody.

Q87 **Baroness Browning:** We have covered quite a bit of my question about definitions. Clearly, we have differing views on the panel. Sir David, in your evidence to the Science and Technology Committee I believe you suggested that somehow you would never get a perfect definition, and in the absence of that a pragmatic approach should be taken. Do you want to identify the balance between being safe and being practical?

Professor Sir David Omand: The starting point has to be the value of communication data both to the police and to the intelligence agencies. The police evidence is very clear. It has

huge importance in ordinary crime as well as in countering terrorism and cybercrime. From that starting point, we have to have an authorisation process that can cope with the number of requests, which is over 500,000 a year, so talking about requiring warrants to be signed by Secretaries of State or senior judges is not appropriate. The justification for that was that it is less intrusive to look at communication data than to look at content, and that principle is reflected in the Bill.

The point I was making to the Science and Technology Committee is that there will be some hard cases, and Professor Anderson gave some examples of precisely that. If you move the cursor too far over to be so restrictive, you create a real problem about the authorisation of data communication requests. If you move it too far the other way, you get the equal and opposite problem of not sufficient authority being applied. The cursor is more or less in the right position, because it has taken the RIPA 2000 definition of who called whom, where and what, and transferred it to the computerised age of which device contacted which server up to the first slash of the address, but there will be hard cases. I was suggesting to the Committee that you have to be pragmatic and ask whether the overall public interest in the authorities and police having this information, which is vital for upholding the law and bringing people to justice, balances the fact that you may occasionally have a hard case. In my view it certainly does.

Baroness Browning: If we get the definition right and if we get the clarity that the panel seems to feel is lacking at the moment, do you think that will serve us for now, or will we have to keep revisiting this?

Professor Sir David Omand: For the sake of clarity, I think the definitions are clear; it is reality that is fuzzy. The parliamentary draftsman has done a very good job trying to clarify this. I am not sure you can make it any clearer.

Baroness Browning: That is very clear. Thank you.

Dr Paul Bernal: This is a really important element. Sir David said that communications data was less intrusive than content. I do not think that is true. They are differently intrusive. There are several reasons communications data can be more intrusive. One is that it is by its very nature more suitable for analysis and aggregation. You can do more processes to it than you can to content. That means that it is subjected to what we loosely called big data analysis. It is also less hard to disguise in some ways. You can talk about a coded, not encrypted, message to somebody. In England we do this all the time; when we say “quite”, it could mean a million different things depending on the context. You cannot do that so easily with communications data. That means that sometimes you can get more information out of communications data than you can from content. I do not think you should be under any illusions that somehow it is okay to have as much communications data gathered as possible but not okay to get content. They are different things. For individuals, sometimes content matters more; en masse, communications data matters more.

The Chairman: Before you came in we were discussing the differences between communications data and content, but the drafters of the Bill and the Government who sponsored it seemed to indicate that there is a significant difference in terms of people’s

privacy with regard to what is written by them and to them, as opposed to the hows, the wheres and the whens, but you are contesting that.

Dr Paul Bernal: I am contesting that. I would say that it can be worse. You have at least some control over what you write, whereas for communications data largely you have very little control over it at all. It is a different sort of intrusion.

Q88 **Baroness Browning:** From the point of view of the speed at which things change, could you indicate whether you think that even if we had an imperfect definition, in your terms, we are going to have to keep coming back to legislation more quickly to update it? Is that a danger?

Dr Paul Bernal: Frankly, yes.

Baroness Browning: Do you think we will keep coming back to this?

Dr Paul Bernal: I think you will be coming back to this and you should be, because things change in so many different ways. This is not the sort of law that you can set down and say it will last for 15 or 20 years without amendment, because the technology is moving too fast; people's behaviour is changing too fast.

Baroness Browning: May I bring you back to Sir David's point? Seeking perfection is perhaps something that we should compromise with pragmatism.

Dr Paul Bernal: You should, but you should compromise it by adding extra oversight rather than by accepting a loose definition, by making sure you can monitor what the intelligence and security services and the police are doing so that pattern of behaviour matches the intent behind the law as well as the definition. This is part of Lord Strasburger's analysis of how powers have grown without parliamentary approval. It is very easy and we have seen it historically again and again. People have not been watching what is going on and you need to continue to monitor things. I am not yet convinced that the oversight arrangements here are strong enough to do that. The idea of, if not a sunset clause, a revisiting clause of some kind might be worthwhile, and also monitoring the monitors: how are the oversight arrangements working?

Q89 **Stuart C McDonald:** Turning to communication service providers and the requirement that could be placed on them to store up to 12 months' worth of communications data and Internet connection records, how feasible is it for providers to do that?

Professor Ross Anderson: It could be extraordinarily difficult and expensive if they are to do what they are advertised to do. We are told that Internet connection records will enable the agencies and police to get past what is called carrier-grade NAT, which is a technique whereby the IP address of your mobile phone might be shared with 1,000 other mobile phones, the idea being that, if someone does a bad thing online on Monday, you ask O2 and they say that it could be any one of 1,000 phone numbers, and, if the person does another bad thing on Wednesday, you have another list of 1,000 phone numbers and you say, "Aha! The common number on the two lists is this one". It is not going to work that well, first because you will find hundreds of common numbers on the list; and, secondly, if you want to relate that to things people have done on other service providers, you have to

relate it to an ID on Google, a handle on Twitter or a logon for Facebook. For that, you would have to require the communication service providers to store very much more data than they do at present. You would have to get them to store precise time stamps, addresses and so forth, which they will not do.

ICRs will not work as advertised. What they will do is create an extraordinary capability power for investigators to say, "Show us all the websites that these two bad people have visited in the past month and all the other people who have visited the same websites". If you want that capability, which appears to be what is intended, you end up requiring lots of people to store lots of stuff. There is, first, the issue of cost if you are to remunerate communication service providers in Britain; and, secondly, there is the likelihood that service providers overseas will refuse outright because it would be too much effort and energy to redevelop their systems, and Britain is only 4% of the market anyway.

Dr Paul Bernal: The Danes are the people who have got closest to doing this, and I would recommend, if you can, to get one of the witnesses from the Danish abandoned attempt. They ran it for nearly seven years and got almost no useful information out of it, but there was a huge cost, even though they were warned beforehand by the ISPs, as I believe they will be here, that this is not a practical proposition and is not likely to be an effective one.

Professor Sir David Omand: The Committee will discover, if they do that research—I hope they will—that the model the Danes chose is not the model I strongly suspect the Home Office would choose. The Danes themselves are revisiting it at this very minute because they may find post-Paris that it is necessary to go back and look at it.

Q90 **Matt Warman:** I want to talk a little about encryption or decryption. Do you think it is reasonable for Government even to ask communications providers to provide unencrypted material for something that is currently encrypted?

Professor Ross Anderson: There is a power in Section 3 of the RIP Act which allows them to do that. As I remarked earlier, Parliament saw fit to hedge it with very stringent safeguards. Nowadays, it would be much more difficult, because many service providers encrypt stuff by default. They do so not out of any particular malice towards agencies but simply to stop other people stealing their ads and customers. It has just become the commercial default; it is what everybody expects. With messaging services, everybody increasingly expects stuff to be encrypted end to end. The Government of Kazakhstan have recently decreed that everybody has to install the Kazakhstan Government's cert on their machine from 1 January. I predict that if you have an iPhone in Kazakhstan you will suddenly find that none of the services works. That will be worth watching.

Matt Warman: Sir David, do you have any thoughts on whether we are likely to get anything meaningful out of demanding unencrypted data from people who currently encrypt it anyway?

Professor Sir David Omand: Of course, you will be distinguishing between content data and communications data, which clearly has to be delivered in a form in which the authorities can use it. If we are looking at content data, as far as I can see there is no back-door encryption provision in the Bill. The Government have said that they are not seeking it. I know the agencies are not seeking it, so as end-to-end encryption spreads it will get harder

and harder for the authorities to be able to access unencrypted content, even for their highest priority suspects. That is a fact of life.

Does that mean that the authorities should have no power to seek such information, and to do their best in cases where it might be available? That is the approach I would commend to the Committee. It is a power to seek, but I do not think it is in Parliament's power to insist that all encryption can be bypassed, nor would it be a very sensible thing to ask for in terms of the national economy and the need for the Internet to be secure. There will be specific cases where it will make sense and information could be made available, and the Bill should provide for that.

Matt Warman: To be clear, in general you do not see the Bill as providing the back door that people have spoken about.

Professor Sir David Omand: No, I do not.

Dr Paul Bernal: Many of the companies concerned do not share Sir David's view, and that is one of the reasons why some of them are distinctly disturbed by news of the Bill. One other thing that we need to be very clear about—Professor Anderson has already referred to it—is that we do not want to put British companies at a disadvantage, because they are more likely to be subject to the force of British law than a company in California or Korea. If we put the power in place to allow them to do it, they are disadvantaged, and that is not good for anybody.

Matt Warman: Which only emphasises the need for clarity, does it not?

Dr Paul Bernal: Clarity is what is needed.

Q91 **Matt Warman:** To move on to equipment interference, what does the panel understand that to be?

Professor Ross Anderson: It is basically hacking or the installation of malware, or what the NSA calls implants and what we call remote administration tools in a machine. If I am a bad person, the police would be able to say to O2, "Put an update on the android on Professor Anderson's phone", and that would enable them remotely to turn it on, use it as a microphone or room bug, or look at me through the camera, collect my location history and all the rest of it. What is more, as we get digital stuff in more and more devices they could do the same to my granddaughter's Barbie doll; they could do the same to your car or your electricity meter. It is open season on the Internet of things. It goes without saying that the controls around that need to be very carefully drawn; otherwise, it undermines trust. If UK producers of stuff can have their arms twisted to provide a capability to put implants into stuff, why should people buy stuff from Britain?

Professor Sir David Omand: I agree with the point Professor Anderson makes about the need for careful oversight of this, but the power already exists; it is already in use under existing statutes, including the 1994 Act. It is of inestimable value to the intelligence agencies, particularly on national security addressed to targets overseas where there are

legitimate demands for intelligence. Some 20% of GCHQ's output benefits from that kind of technique. There is nothing very new about it.

Dr Paul Bernal: There is nothing new about it, but there is something new about our behaviour and the technology we all use. Twenty years ago I was not using anything that was encrypted at all; now half the stuff I have on my phone is encrypted by default, and another batch is encrypted by choice by me, so for normal people this now becomes relevant when it was not relevant before.

Professor Ross Anderson: What is new is that we found out about it thanks to Edward Snowden, and GCHQ admitted that it was doing it just in the last month or two, thanks to the case currently before the Investigatory Powers Tribunal. People are beginning to get worried about it, and with due cause.

Q92 **Lord Strasburger:** Gentlemen, can you help me out with bulk personal datasets? The Bill and the Explanatory Notes are very vague about that. The ISC report was rather vague about it—it was hugely redacted. The Home Office will not tell the Committee the identity of the databases it is scooping up, so it is very difficult for this Committee to assess the proportionality, risks and intrusiveness of the collection of bulk personal datasets. Does anybody know what they contain? Do they contain medical records? Do they contain bank records? What do they contain?

Professor Ross Anderson: For starters, we know that the police have access to things like credit reference and DVLA records. That is public knowledge. Secondly, they have access to medical stuff. They have had that since 1996. At the time, I happened to be advising the BMA on safety and privacy and that sort of thing came through. Thirdly, in any case, hospital medical records were sold on a wide scale in the care.data scandal last year, and it would have been rather negligent if GCHQ had not grabbed a copy on its way past. Fourthly, it is well known that some kinds of bank records, in particular all international financial transactions, are harvested on their way through the SWIFT system.

Professor Sir David Omand: Not true.

Professor Ross Anderson: This has been a matter of enormous contention in the EU and elsewhere. It is only to be expected. If I were, for example, an investigator for the FCA, I would want everybody's bank statements too.

Professor Sir David Omand: Chairman, it is important not to allow fantasy to intrude at this point. The central bank governors responsible for the SWIFT system agreed that that system could be searched for specific transactions of known criminals and terrorists. That is public knowledge. All SWIFT data is not scooped up.

Lord Strasburger: Perhaps we could impress on the Home Office the need for the identity of these databases to be revealed.

The Chairman: That is something that we would have to do in private session, but I take the point that there is a serious difference of view between the witnesses on what is a hugely important subject.

Q93 **Dr Andrew Murrison:** I am going to be fairly brief, because I think we have covered quite a lot of this already. I refer to the international dimension. We sit here thinking we can make various laws and regulations, but we are talking about a global industry. Referring to some of your previous comments, could you reiterate the likely reaction of the international community to the Bill, in particular the feasibility of gathering ICRs, given that it is entirely in the gift of companies whose headquarters are not in the UK?

Professor Sir David Omand: We took evidence on this as part of the independent surveillance and privacy review run by RUSI and we got a variety of answers from international and British companies. Some of the companies said that as a matter of corporate social responsibility they wanted to be in a position to provide this kind of information for the purpose of preventing serious crime and terrorism, but they felt extremely nervous about doing it without a firm legal basis on which warrants or authorisations would be made. Other companies said that as a matter of company policy they did not believe their data should be made available to any state or law enforcement authority. You have a variety of views. The provisions of the Bill, which include the provision that the Home Secretary can make judgments about what it is reasonable to expect, will be partially successful; but they will not be completely successful, because some companies will simply refuse, and I cannot see the British Government attempting to launch civil actions against major players.

Dr Andrew Murrison: Presumably that means that the disinclined would note those who were complying and those who were not and go for those who were not.

Professor Sir David Omand: The intention is not to make public the companies that comply and those that do not.

Professor Ross Anderson: We all know the companies that will comply. They are the ones that get large amounts of their revenue from Governments, or that rely on Governments for capture regulators—companies such as IBM, BT and those set up several generations ago. Companies that have been set up in the past 20 years think differently because they have a different culture—the Silicon Valley culture. Their money comes either from their users directly or from advertising—from their users buying stuff or being advertised to—and they take a completely different view. It is not much good getting BT on board if all BT is doing is providing a piece of copper wire from people's houses to where the real action starts, so it is the view of the big American service companies that matters more than most. They are going to drag their heels.

There is the issue of foreign Governments. There is also the issue of what happens to small start-ups in the UK, which is absolutely crucial. For example, about five years ago one of my postdocs set up a security start-up. Because of the arm-twisting that the agencies have always indulged in, he decided to set up a coding shop in Brno in the Czech Republic. More and more people will be doing that, simply as a matter of default. You cannot run a tech start-up nowadays unless you have a marketing operation in North America, because that is where you make your first sale and most of your initial sales. If we create a regulatory regime where it is only common sense for people to put their coding shop, their

engineering, in North America, Seoul, Mumbai or wherever, the cost to us directly or indirectly down the stream of time will be huge.

Dr Paul Bernal: We have to be aware of where things are moving. There may be a number that are co-operating willingly now, but that will shrink. More and more companies are likely to say, "No, we are not going to give this", and they will be the bigger and more successful ones. You make yourself a hostage to fortune by assuming that this will end up functioning.

The Chairman: Thank you very much indeed. I thought the whole session was absolutely riveting. You have given us an enormous amount to think about. Obviously, you have very different and varying views on the issues before us, but you highlighted issues that very much need highlighting. I know that members of the Committee are grateful to all four of you for giving us your very robust and significant views on this important Bill. If you would like to add any written evidence to supplement what you have said, we would be more than happy—indeed delighted—to receive it. Thank you very much indeed.

Jim Killock, Executive Director, Open Rights Group (QQ 127-136)

Evidence heard in public Questions 127-136

Oral Evidence

Taken before the Joint Committee

on Wednesday 9 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Lord Henley, Lord Strasburger.

Witness: **Jim Killock**, Executive Director, Open Rights Group, gave evidence.

Q127 The Chairman: A very good afternoon to you—or evening, now. I am sorry that we are a little late—there was a vote in the Commons earlier. You are very welcome. I will make two points before I ask the first couple of questions. My colleagues will come in after that. Each of you has given your response to the Bill very publicly over the last number of weeks. The Committee has all the statements that you have made. In addition, of course, I am sure that you will give us written evidence. This is a very big Bill. It is very lengthy and very technical. Has subsequent analysis of the draft Bill led any of you to alter any of your positions from those that were taken in your initial response to the Bill's publication?

Shami Chakrabarti: I would simply say that I am possibly more alarmed by the Bill than I was at first glance. The Committee will appreciate that it is a long Bill.

The Chairman: Very long.

Shami Chakrabarti: It is very complex. Like all legislation, it requires an understanding of what its clauses actually provide, as opposed to how its clauses have been pre-briefed or spun in the press. It also requires a level of understanding of the relevant technology. Those two things have to come together. My own organisation is a human rights organisation with, traditionally, considerable expertise in legislation, but recent weeks have given us the opportunity to work with partner organisations that have a considerable level of expertise in the technical sphere. That experience makes me more alarmed now about the personal and cybersecurity implications of the provisions, however laudable and well-meaning they may be in their motivation.

The Chairman: Do your colleagues share that view? Are you more alarmed now, as the weeks go by?

Renate Samson: Initially I was very clear that there was a lot to read. I have now read through it. The implication was that there was a lot of transparency. At first, it seemed that that was the case, but, as you read more and more, you find that there are a lot of vague terms in the Bill that require a lot of head-scratching to try to understand exactly what may be meant. Trying to engage the public in understanding what the Bill says and what its

implications for them will be has been a challenge. There probably need to be many more readings of the Bill before you can get to the bottom of even a tip of what might have been meant.

Caroline Wilson Palow: I agree. We did and do welcome the opportunity to engage in this process. As we have started to get into the Bill, which is long and complex, we have started to notice a few things. For instance, Part 6 is about bulk powers, but when you look into some of the other particularly targeted provisions, you start to see that aspects of those look quite a lot like bulk powers in and of themselves. The service provider provisions that are sprinkled throughout the Bill put a lot of obligations on service providers, which I know you have often heard about, and which seem like they could undermine both security and trust. Those were not things that were necessarily apparent when we first took a look at the Bill. Another particular provision that concerns us a bit is Clause 188, on national security notices, and how that will play out in conjunction with the other provisions of the Bill.

Jim Killock: We have been particularly alarmed by the reintroduction of the so-called filter, which complements the collection of very widely defined Internet connection records. The filter seems to us to be essentially a federated database and search system, very much like previous incarnations of the Communications Data Bill, the snoopers' charter or the intercept modernisation programme. It has been proposed a number of times and stopped a number of times, because of the power to look into people's lives that it would give. In a sense, that deserves an entire debate on its own, as does the recent admission of collection and use of bulk datasets.

What is a bulk dataset? Which of them have been accessed and grabbed by GCHQ so far? To whom might that apply? Just about every business in the country operates a database with personal information in it. It could be Tesco Clubcard information. It could be Experian's data about people's financial transactions. It could be banking details. It could certainly be any government database that you care to mention. From that perspective, it is hard to see where surveillance ends as a result of bulk datasets. Traditionally, we have thought of surveillance as being about communications data and as being targeted. In this Bill, we have various measures for blanket collection—bulk collection, as it is referred to—and we extend that to any private or public institution that happens to have data. From that perspective, it is pretty worrying. It is hard to see the start and end of it.

One good thing that we did not necessarily expect is that there is a thorough or, at least, a large document spelling out the apparent operational case for Internet connection records. The fact that that has been produced is a welcome step. A very important thing to do when asking for a new power is to produce documentation explaining why it might be needed. That said, it again requires examination on its own behalf, as do the GCHQ powers. They need an operational case. Parliament has not debated why GCHQ has those powers; it has merely been presented as something that is happening and that we should now legitimise. In the USA, those kinds of powers were examined—bulk data collection and use under Section 215 of the Patriot Act. An operational case was made and was reviewed by bodies that were trusted by the President and by the USA's democratic institutions—the Privacy and Civil Liberties Oversight Board and the NSA review board. Both came back and said that there was no operational case for the bulk collection and use of data; nothing the NSA had done showed that that data had prevented anything significant. That kind of review needs

to happen here. The fact that it has happened in the USA and they have come up with the conclusion that these programmes need rolling back ought to be something that you consider carefully. Parliament really needs to examine those operational cases.

Q128 The Chairman: I think that I have got the message. I am assuming that you do not think that the Bill strikes the right balance between security and privacy. Without going into detail—my colleagues will ask questions on different parts of the legislation—other than dumping it altogether, do you think that it could be improved?

Shami Chakrabarti: It could certainly be improved. One thing we would all agree on, and would agree with the Government on, is that there needed to be a new Bill, in the light of Mr Snowden's breathtaking revelations. Whether you consider him a hero or a traitor, there is no doubt that he revealed practices and capabilities where we, the people of great democracies on both sides of the Atlantic and all over the world—I would include parliamentarians in that definition of the people—had little or no idea of the sheer scale of mass surveillance that was being conducted against populations. There is a debate to be had, of course, about how much of that should or should not happen, on what basis and with what safeguards, but in the light of that there had to be new legislation, because whatever was happening was happening, at best, on very creative interpretations of outmoded laws. Some of us would suggest that it was happening outside the law and without sufficient parliamentary scrutiny, public discourse and legal authority.

We certainly agree that there must be a new Bill; there must be something like this Bill. My fundamental objection is that too much of it is about sanctioning mass surveillance of entire populations and departing from traditional democratic norms of targeted, suspicion-based surveillance, for limited purposes. There are insufficient safeguards against abuse. For example, there is the argument that I know you have had extensively about the role of the judiciary. Our position is clear. This is not a system of judicial warrantry. This is Secretary of State warrantry, save in one of the most chilling provisions of the Bill, which is about hacking and the new concept in public understanding of what the authorities propose to do. We think that is one of the gravest powers, because potentially it leaves long-term damage to systems, individuals, devices and security, after a perhaps justifiable investigation. That has the lowest safeguard of all, because in certain circumstances it involves not even the Secretary of State but, for example, a chief constable. There is too much surveillance, there are too many people, it is not to a tight enough threshold or a high enough standard and there is insufficient authorisation by the independent judiciary.

Caroline Wilson Palow: Following on from that and your introduction to the question, security and privacy are not necessarily mutually exclusive. The hacking provision, in particular, shows that there is a lot of potential to undermine security by allowing that power, including the fact that the use of malware—the type of software that allows access to computers through hacking—is not necessarily well controlled. It is like breaking a lock on a door and leaving the lock broken, so that other people can potentially get in and access the same device or equipment that was targeted in the first place. That is an example, within equipment interference, of some of the security problems. There are also greater, overarching concerns about undermining things like encryption standards and whether or not that would be permissible, both under the hacking provision and under some of the provisions, like Clause 189, which say specifically that the removal of electronic protection could be required of service providers that are subject to compliance with warrants and

authorisations under the Bill. Finally, data retention in and of itself has certain security concerns. Of course, as we have recently seen with TalkTalk here or even the Office of Personnel Management in the US, there are breaches. When you are mandating companies or even Governments to keep more information, it makes the breach even worse when it happens.

Renate Samson: I support the points that have been made about concerns with regard to safeguards. Caroline made the point that privacy and security are two sides of the same coin. We also have to look at the idea of protection. Part of this Bill is about protecting the public, yet, as has been pointed out, there are other elements that will potentially make the public vulnerable, whether that is through equipment interference or through weakening of encryption, for example. We have to step back and have a think about what protections the public require with regard to the proposals in the Bill. The idea of full independent judicial authorisation is something that I know you have been discussing at length. I would support the view that it needs to be explored in a lot of detail. We are on the cusp of being complete digital citizens. We do not have a choice any longer about our engagement online. Proposals that suggest that online engagement can be surveilled at any time, potentially, and retained for a number of months are a worry to us all. It is not the case that the Bill should be scrapped, but there are certainly areas that need to be strengthened greatly.

Suella Fernandes: On the flipside of those comments, do you equally accept that the scale and nature of the threat that we currently face is unprecedented and severe?

Shami Chakrabarti: I do not doubt that the world faces enormous threats from crime, terrorism and so on. I do not think that any of us doubts that. The question is how best to counter those threats. I will repeat the previous remarks, which are really important. It is not about a trade-off between privacy and security. A lot of what we are concerned about is actually security. What is national security if not the personal and, increasingly, the personal cybersecurity in relation to where I am—whether somebody is in my house, engaging online, and whether I am away and, therefore, open to an attack or a burglary? My financial records and so on are part of my personal security and cybersecurity. National security is to some extent the combined personal and cybersecurity of millions of people. We think that up to 50 billion emails are intercepted every day by UK authorities. There are only 7 billion people in the world, and only 3 billion of them currently have access to this kind of technology. To me, that in itself is a threat to personal security—not because the authorities are malign, but because when you collect data and create vulnerabilities, that data can be attacked by non-governmental sources and the vulnerabilities that have been created can be attacked similarly.

Suella Fernandes: On the vulnerabilities you talk about, you point out the scale of, for example, communications data and equipment interference and interception, but those powers have been absolutely essential and critical to successful convictions for large-scale child sexual exploitation, human trafficking and serious and organised fraud and crime. Those are powers that are currently exercisable by our law enforcement services. The Bill represents a drawing together and consolidation of existing powers.

Jim Killock: We are talking about several different things here. There are policing powers, there are data retention powers and there is extension of those for the police in the ICRs and the filter, so you have that body. Then you have the other area around GCHQ—what it does and how it gathers information. You have to look at both of those quite separately.

You are really asking about the operational case. As I said, my problem with the operational case is that it has not been presented to anybody for GCHQ. When the equivalent was done in the USA, the President of the USA and its democratic institutions decided that there was not really a case for a lot of it and decided to roll it back, because it was essentially purposeless. Here we have an operational case for the police with regard to ICRs, but we do not have the mechanisms, because we do not have a civil liberties board in the UK. It has not been constituted, despite potentially being put into law. That has not been examined.

On data retention in general, we have had a ratcheting back of data retention in a lot of Europe. These apparently essential tools have not been operational for a long time in Germany, the Czech Republic, Slovakia and a number of other places. There are about six or seven countries where these sorts of programmes have essentially been cancelled. There has not been a concomitant outcry from the police that they are no longer able to solve crimes and that there is spiralling dysfunction in the police. That has not occurred. Something to bear in mind is that there are often several routes to solving crimes. Data, through data retention or collection, is only one. That data probably resides on laptops and mobile phones. It will reside at service providers. That is talking only about the data side of it; there will be other kinds of factors in the equation. It would be interesting to hear from Caroline about data preservation and the standards elsewhere.

Caroline Wilson Palow: The US, for instance, does not have a data retention provision, yet it is still able to solve crimes. In fact, it uses mechanisms like data preservation orders, which are much more targeted, are not across the board and can be quite effective. You also have instances, which have been mentioned, of places like Germany, the Czech Republic and other countries in Europe where data retention is either much more circumscribed or non-existent. Again, we have not seen a collapse due to the fact that it is not there.

To pick up another point you asked about—the existing powers, particularly in the context of equipment interference—it is true that it was revealed earlier this year that the intelligence services were engaging in hacking and, when this Bill was introduced, that law enforcement, too, was engaged in hacking. Until that point, that had not been revealed publicly. The reliance on the Intelligence Services Act and the Police Act, which are incredibly broad powers, to say that that was already in statute is inappropriate, because they are so broad. There was no indication that it was actually happening. Since those Acts are from 1994 and 1997, if there was an indication in the Acts that hacking was possible, why was there concern not to reveal it sooner? Why was the position of the Government until earlier this year neither to confirm nor to deny that those powers were being used? While they may have been in use, they have not actually been in law up to this point. That is why we talk about them as new powers in this Bill.

Shami Chakrabarti: I have one further small point on comparative practice around the world and the importance of law enforcement. There is still no provision for intercept

evidence to be admissible in criminal proceedings. There has been and is to be all this interception, for laudable criminal justice purposes—public protection and law enforcement—but there is still not the provision, for which some of us have asked for many years, for interception, when it is proportionately and lawfully gained, to be used in criminal prosecutions, as is the case all over the democratic world and among our allies.

The Chairman: Thank you. I move to Dr Murrison.

Q129 Dr Andrew Murrison: I am getting the sense that you are not convinced that the "double-lock" provision, about which much has been spoken in recent weeks and on which much store has been put by those who have been involved in bringing the Bill to the position it is currently at, is really much cop. However, I believe that it is likely to remain a feature. Given that it is likely, what do you think could be done to improve the double lock? Would you see virtue, for example, in distinguishing national security from serious crime, having the double lock apply to national security and having judicial authorisation only for serious crime? Would you see virtue in, for example, a different means of appointing the information commissioners who will be involved in this process?

Shami Chakrabarti: Some of my colleagues are the great technologists and experts. I am just a humble lawyer in recovery—or in remission—so I find it easier to make the analogy with the real world when I am dealing with the virtual one. We are digital citizens, but we are still people and citizens. If I want to search your house or your office for laudable reasons, I go to a magistrate for a warrant. I can understand the argument coming from the Government that when we are doing this national security stuff and, perhaps, spying on foreign Governments, we cannot just go to any old magistrate. There has to be a double lock, surely, on something as serious as interfering with the German Chancellor's communications. That is such a political decision that there ought to be some Executive involvement. The double lock is simple: have a provision across the board for judicial warrantry, but as an internal administrative matter, make sure that those warrants are not sought by the authorities unless they have been to the Home Secretary first. In the non-crime cases—the international relations/national security cases—as a matter of good public administration, go to a Secretary of State first, but always have the sign-off to protect people's rights and freedoms, whether in the UK or around the world. Have that sign-off by a judge, as you would for your home, your flat or your office. Again, that is the practice across the democratic world.

Renate Samson: I second that. A large part of what we find ourselves doing when it comes to the digital world is incomprehensible to most of us, because it is invisible, yet we all understand what happens when somebody knocks at our door and asks to have a look around because they suspect us of something, and that element of being suspected of something is important. The real world understands a judge signing off on something. The general public have confidence that there is independence to it. While we may currently have a benign Government, we do not know what the future holds. This piece of legislation should hold up for many years. We do not know what the future will bring, so independence is hugely important. That will also mean how the judges are appointed. To feel genuinely that surveillance conducted upon us is being assessed independently and with no interference from anywhere else will reassure the general public that, should the

rest of the provisions in the Bill become law, they will be secure and thoroughly thought through, not just signed off with a flick of a Minister's pen.

The Chairman: It is said that a Secretary of State is ultimately accountable to Parliament for his or her actions, whereas a judge is not. What is your view on that?

Renate Samson: You took evidence at the beginning of this week from Mr Paterson and Lord Blunkett. I think that they answered that question for you, in that neither of them has ever stood up in Parliament and talked about a warrant they have been involved in signing off.

Jim Killock: It is also worth reminding ourselves how we got here, in a sense. The Regulation of Investigatory Powers Act had powers for the collection of material from persons overseas. The meaning of that warrantry system was extended through practice to mean every communication passing between the UK and the USA. That is how the Tempora system of bulk collection was created—through those warrants, which were politically authorised. There was a political decision, alone, to extend the meaning of those RIPA warrants, which meant that essentially Parliament was cut out of the decision, right or wrong, to engage in the programmes of bulk collection of data that we are now authorising in this Bill. It seems to me that if one is to restrain the Executive from creative interpretations of the statutes, as Shami said, you need that judicial authorisation. They should be saying, "Minister, I do not think that this is necessarily how the system was designed to work. Perhaps you might like to consult Parliament". That is a far more likely outcome than the Home Secretary saying to GCHQ, "No, I am going to deny you those powers for one or two years while I work out a political opportunity to legislate".

Caroline Wilson Palow: In conjunction with that point, it means that the judicial commissioners need the full ability to assess the warrants when they come to them. It should not be just a judicial review standard. They need to assess fully the substance of the warrant and, among other things, whether there are other less obtrusive means by which this information could be obtained. That is an easy edit to the Bill. Every time the judicial review provisions appear—it is at subsection (2) of most of those clauses—you just delete it. You take it out.

Suella Fernandes: Are you saying that the double lock and the judicial involvement strike the right balance in having judicial review as an element of the decision-making process, or are you saying that it should not be there?

Shami Chakrabarti: Judicial review does not help at all in this context. When you are deciding whether it is proportionate to issue a warrant for intrusive surveillance of an individual, let alone of a whole group of people, that is a judgment made on the evidence. A judicial review test only second-guesses the Secretary of State, in very limited circumstances. Did they make a bonkers decision that no reasonable Secretary of State could take? That is not judicial warrantry. In the statute there should be a one-stage test: the judge signs the warrant. However, because people are concerned about cases of interception on foreign powers, for example, which is classically a matter for the Executive rather than for independent judges, police officers or whatever, interception and so on of foreign statesmen and powers should go to the Home Secretary first, as a matter of good

public administration. You would not even need that in the statute, or you could put it in the statute for that category of case.

Renate Samson: Your question is interesting. I have listened to a number of the sessions of evidence that you have taken. You have all posed the question a number of times, "What exactly is meant by judicial review?". Witnesses have given you a variety of versions of what judicial review means. There is lack of clarity.

Suella Fernandes: That is exactly what I was going to raise in my question. You will agree that, with judicial review, the judge would have access to the same information as the Secretary of State or the Minister.

Shami Chakrabarti: I do not think that is suggested in the Bill. There is nothing to suggest that.

Suella Fernandes: That is what judicial review involves, does it not?

Shami Chakrabarti: No, it does not. This is a term of art. A judicial review test, as a matter of our law, is a very limited opportunity for a judge to second-guess a decision that has been made by a public authority, whether it is a Secretary of State, local government or whatever. It is not a double lock.

Jim Killock: Basically, it is, "How did you follow procedure?", is it not?

Shami Chakrabarti: Yes. Did you make a decision that was within the realms of a reasonable decision? Could any reasonable Secretary of State possibly have made that decision? It is not appropriate for warrantry.

Suella Fernandes: What about the proportionality test, which involves balancing the right infringed and the objective met? That goes further than what you are suggesting, does it not?

Shami Chakrabarti: But that has not been allowed to the judge, under the provisions of the Bill. They are not second-guessing the Home Secretary's decision on the merits of proportionality, under the Bill.

Caroline Wilson Palow: That is exactly our concern. When you talk about judicial review, all you are doing is looking to see whether proportionality has been assessed by the Secretary of State. The judge will not have the power to say, "You have made that assessment incorrectly". In the US, to give an example of a comparison between two different types of warrantry there, a normal warrant would go directly to the judge. There is a political consideration that is made ahead of time. For instance, the US attorneys, who are the federal attorneys who often start the process, are politically appointed and will make a decision about whether or not to seek a warrant in the first place. Once that is done, it goes directly to the judge.

Suella Fernandes: Before we finish this line of questioning—I know that other people want to get in—I need to put on the record that the statute states explicitly that it must be "proportionate" and "necessary". That is the relevant test.

Shami Chakrabarti: You have to look at Clause 19(2).

Caroline Wilson Palow: The concern is the way in which the two play together. That is why I said that we think you should just delete subsection (2). We totally agree that necessity and proportionality need to be assessed, but, once subsection (2) is in there, it reduces the ability of the judicial commissioners to make that assessment. To continue the parallel that I was trying to draw, in the US there has been a lot of talk about the FIS Court, which acts on foreign intelligence. This is PRISM—the types of authorisations for collecting intelligence on people around the world. Its powers are the equivalent of what judicial review would be here. Essentially, when a request comes to it, it has to check the box to say that everything has been considered as necessary, but it does not necessarily get to question the conclusions that were reached by the person who was seeking the warrant in the first place.

Shami Chakrabarti: A double lock would mean, "I can substitute my decision on the merits for yours". Traditional judicial review means, "I look at the way you made your decision, but I do not substitute my own for yours". You have to be procedurally irregular or to have made a completely insane decision that no Secretary of State could make. That is achieved by Clause 19(2), otherwise there would be no purpose to it.

Matt Warman: We have had an awful lot of witnesses tell us that their expectation and understanding of what the Bill says regarding judicial review would, as Suella Fernandes has said, in fact mean a test that looked at the evidence. It would have to be proportionate and go through all those things. You are saying simply that that is not your understanding of judicial review. It therefore seems to me that we are talking simply about definitions; we are not actually talking about a principle, because what we have been told is what you are saying you are asking for.

Shami Chakrabarti: It just does not stand up in law. These are well-tested terms. If you want to create a full merits appeal in statute, there are many precedents for doing that. You do not put in a clause like 19(2); you can do it much more simply. I believe that you will hear from the Secretary of State in the not-too-distant future. You can just ask her: "Is it your view that you will make an initial decision and there will be a full merits review? The judge can just second-guess your decision and make a different one. Is that your intention?". If she says that that is her intention, that will help for Pepper v Hart purposes, but there are far clearer ways to deal with it, like just deleting Clause 19(2).

The Chairman: Thank you. Can I move to Mr McDonald?

Q130 Stuart C McDonald: I have another million-dollar question. What is your understanding of the meaning of the term "Internet connection record"? Why would their gathering and analysis be more intrusive than for other forms of communications data?

Shami Chakrabarti: This has been quite a journey for me. I have had lots of younger and more technologically savvy colleagues explain the sheer scale of what we might be looking at as regards Internet connection records. If you take your favourite device—your smartphone, your tablet or just the sites you go to from your laptop or desktop—we are looking at things like the websites you visit. We are looking at the communications software that you might use to speak to your mother—Skype, WhatsApp and so on. We are looking at all the icons on your menu, such as your Twitter and your diary. Recently a health one popped up on my phone uninvited, telling me how many steps I took yesterday. Taxis,

maps; the list goes on. Photos, my Internet shopping, banking apps—I understand that all those things are potentially within the broad concept of Internet connection records. As we look just a little way into the future, in the discussion that people describe of the Internet of things, more and more of our real lives will be managed online. Now we will be talking more and more about the little icons on our devices that connect to our fridges, our cars, our burglar alarms, our gaming devices and so on, so the separation between my real-world security and privacy and my cybersecurity and privacy is almost completely collapsed. This is very intrusive on millions and millions of, for the most part, completely innocent people.

Renate Samson: It comes back to the point that I made that we are all now digital citizens. It is that—it is life. It may feel at the moment that it is just a mobile phone and a laptop, but, as Shami explained, with the Internet of things it will be everything. That will create a huge amount of data that will be constantly ticking over. We have been informed that the Internet connection records are just the URL, before the first slash, of a website and no content, but from the technical evidence I have been listening to and you have been receiving, and from all the different things that I have read, which Jim will probably be able to explain better, I am not entirely sure that it is quite as clear-cut as has been implied. I would certainly like to hear from the Home Office—from government—with regard to this Bill a very clear definition that it knows exactly how this can be done, because I am not sure that I do.

Jim Killock: It seems to me that essentially the Internet connection record starts from the point of view that the Home Office wants the power to have retained the fact of somebody using the Internet, with some other service, and to record that. It has decided that the best way to do that, given how much the Internet is used, the purposes it might be put to in the future and the services that might appear, is just to say, "Let's have a very broad definition of anything that connects to anything, whether it is a person or a machine. That will allow us to compel Internet service providers to collect information about anything we deem important in the future".

I do not think that is really a good way to legislate. It is incredibly broad, it is open to abuse and the cost implications are impossible to put a number on. If you have power to collect and retain any information, no matter how difficult that is and how much of it there is, essentially you have just written a blank cheque to scale up surveillance indefinitely. Of course, once you have an initial investment and the thing has started to roll out, that poses the problem of how you restrain it in the future when it turns out to be not quite as useful as you hoped. Do you pour in another few tens of millions of pounds to extend the amount of information that you are collecting under this very broad power? Given that the companies will probably tell the Government that it will be more effective if they spend that extra bit of money, this seems to be a financially haphazard way of working, as well as haphazard in terms of human rights and the proportionality of the surveillance we are authorising.

Caroline Wilson Palow: This is quite a confusing definition, because essentially you have two different definitions in the Bill. You have Part 3, where Internet connection records are explicitly mentioned, but in Part 4, under data retention, you have a clause that, under the commentary, is supposed also to encompass Internet connection records. The definitions

do not completely align, and for that reason we are somewhat confused about what Internet connection records really are.

Let us take an example from the commentary that Renate has already mentioned—the idea of taking the domain name of a website, which is the information before the first slash. Potentially, that could be quite intrusive and could reveal a whole lot of information. It is not as innocuous as just bbc.co.uk, which is the example that they gave. For instance, that domain name could be saveyourmarriagelikeme.net or domesticviolenceservices.com. Maybe one of the most interesting ones is crimestoppers-uk.org. This is where you can make anonymous tips to help to solve crimes. Of course, if you had the Internet connection record that said that someone had gone to crimestoppers-uk.org and you also knew the time when the tip had come in—if you were the police, for instance—you could very easily figure out who had put in that tip. That is a real problem, because if you are destroying that anonymity you can undermine the ability to solve crime.

Q131 Mr David Hanson: This is the central question many of us will have to wrestle with. Surely the police, the security services or whoever accesses that, under authority, with judicial review, is doing so only because there is some potential link to a potential investigation. The vast majority of people will never have that link checked or looked at. I am wrestling with that myself. I want to get your assessment of whether the proportionality is there. If we do not collect the information, none of those leads can be followed up.

Shami Chakrabarti: You are collecting huge amounts of sensitive information that is not currently collected and, therefore, you are creating the vulnerability I am so concerned about. I am not even talking at the moment about potential abuses by the authorities. I am talking about the vulnerability to hacking by other people that you create when you create a massive sensitive database and put the entire population's online life under surveillance in this way.

Renate Samson: My understanding is that this would help to support requests that are already made for communications data. At the end of November, IOCCO published as a starting point to a further publication a breakdown of 100,000 communications data requests by 29 police authorities, including the National Crime Agency; 46% of those requests related to burglary, robbery, theft and drug offences. If this is to support that, people may see it very much as an intrusion. On that sort of issue of crime, why do you need to know what website somebody has looked at with regard to burglary? We have to think about the intrusion into people's lives, based on us as digital citizens, before we start to discuss the retention and use of Internet connection records. Their retention is an issue I know you have looked at, but off the back of the TalkTalk hack, for example, we need a lot more clarity on how companies will be asked to store that data to ensure that they are safe.

Jim Killock: You also have to consider the wider effects on society. If I said to you, "When you go home, can you note when you got home and which newspaper you read, although do not worry which article it was? If you ring your family this evening, make a note of that and then tomorrow, hand it into the police", you would think that an excessive ask.

Shami Chakrabarti: And every hotelier, every restaurant owner, every pub, every cinema and every theatre that you enter will be required to keep a record of when and where you entered. That is the equivalent of what is being proposed.

Jim Killock: The question then is, is that a proportionate thing? What are we trying to solve? Is it quite as desperate a situation as is being claimed? As I said, these powers do not exist in other democratic countries. Russia has just been given a bit of a rap for similar sorts of activity. A number of European countries have rolled back on traditional data retention, never mind this kind of extension.

The Chairman: Lord Strasburger?

Lord Strasburger: My point has just been covered.

Q132 Stuart C McDonald: Are there other ways to go about IP resolution that are less troubling? The Home Office and law enforcement agencies will say that retention of these connection records is essential for that to be successful.

Jim Killock: One thing that you have to ask is whether the technology will out-evolve this. Will IPv6 catch up with some of the problems that it is currently seeing? You also have to ask how the Internet might work in the future and whether any of this will work. Some of the evidence that has been put about is quite interesting. People have said, "How do we know whether somebody has used Twitter or Facebook? We need to know in emergencies whether somebody has been accessing that website". Phones just do that now every couple of minutes. If they are constantly connecting to all these services, you will just have a huge glut of information that is not a fat lot of use to anybody.

Q133 Matt Warman: One of my frustrations with this conversation is that it is always said that the Government are being asked to hold this stuff. Actually, we are asking ISPs to hold it. That is a very important distinction that we need to continue to make. Law enforcement agencies tell us that they want access to the information and are happy for it to be held externally. You seem to be saying that you are not happy with that. I wonder what alternative you would propose.

Jim Killock: It may not be a government-held database, but it is a series of data centres that are all accessible by a single mechanism that can then be queried in parallel from an officer's desk.

Matt Warman: With appropriate oversight.

Jim Killock: There are some interesting things there. It seems that the way it will work is that you can get an officer to ask the computer whether it has any useful information in a case. It will tell you the things that it might have, and then you can go off and get some warrantry for it. It is almost saying, "We will go not on fishing expeditions, but if you did, here are the results you would get. Why don't you have a think about whether or not that is useful?".

Renate Samson: You say that there will be appropriate oversight. Currently the Bill will retain the process that we have now. From Big Brother Watch's point of view, that is not

appropriate oversight. We would like to see a further layer of independent judicial approval and authorisation of an internally signed-off warrant.

Matt Warman: The point I was making is that it is not a free bucket any policeman can look at.

Renate Samson: We also have to acknowledge the recent case with regard to Police Scotland and on which IOCCO reported, where warrants were being signed off and misused.

Matt Warman: Misused being the operative point.

Renate Samson: Yes.

Shami Chakrabarti: Sometimes that will happen. To go back to the real-world analogy, when I said that this is the online equivalent of requiring all those businesses—hoteliers, restaurants, cinemas and so on—to keep a detailed record that they do not currently keep of everybody's comings and goings, that does not mean that I am against ever putting a particular hotel, restaurant, gym or whatever under surveillance. I just think that you take a targeted approach. When you get suspicion that conspiracies are being conducted in a particular room above a particular pub, at that point you put that site under surveillance. Then you put the people who have been to that site under surveillance. That is the kind of approach we should continue with in our democracy, in the virtual world as well as the real one. If you have concerns about particular activity and sites, you can go to ISPs and CSPs and ask for the data they currently hold anyway. You can seize people's devices, because those people or organisations have now come under suspicion. You can target suspicion not just around individual people but around organisations and, indeed, websites.

Renate Samson: I want to clarify your point about misuse. IOCCO is very clear that judicial approval was not obtained to acquire the communications data. My point, and the point of Big Brother Watch, is that independent oversight and authorisation of an internally signed-off warrant for communications data would, I hope, potentially ensure that misuse did not occur. That is just for clarity.

Jim Killock: The important thing is why we have the idea that necessary and proportionate surveillance is essentially targeted, rather than blanket. Why do we have that rule? Why has that been pushed forward? It is easy to imagine that in the UK we will never have any problems with our democratic institutions, the police will never overstep the mark and we can solve all this through authorisation regimes. However, if you look over the sea in France, you have the potential of a Front National Government, with parallel powers. You have powers similar to these in China and Russia. Is it the role of the UK to say that blanket surveillance, easy profiling and access to everything that everyone does in their lives is the right international standard to set and is absolutely, 100%, guaranteed never to turn into a problem in this country, or should we restrain surveillance to somewhere we can trust, for ourselves, for other people and for the long term?

The Chairman: Can I move to Lord Butler?

Q134 Lord Butler of Brockwell: I want to ask you about equipment interference. You have made reference to that. As I understand it, you are not claiming that equipment interference in the past has been non-statutory. You are claiming that, although there are statutory powers, they are very general, they have been widely interpreted and the public have not been aware of what is going on. Do I have your argument right?

Shami Chakrabarti: You do have my argument right. I do not believe that equipment interference was necessarily in the mind of the legislators when the provisions that are now being relied on were passed. Those provisions were more about traditional breaking and entering, bugging and so on. I certainly do not think that the public understood in that way the activity that was being justified ex post facto. That creates a problem for Article 8 of the convention, which requires a certain level of public understanding for something to be law for the purposes of the ECHR. Those powers were there and they were used for more traditional interferences, but hacking is a very, very serious business. It is more than just surveillance, because you are potentially changing data and causing long-term damage to data security. I am not saying that it should never be allowed, because that would be like saying that you should never break and enter in order to find the hostage, the terrorists and so on; I just think that there should be much tighter safeguards for hacking in the Bill. Again, in principle, it should be a targeted approach, not a blanket one.

Jim Killock: It is worth remembering that the hacking power has already caused some very significant problems. You probably remember that Belgacom, the telecoms provider in Belgium, was hacked by GCHQ, allegedly. In the first month of the clean-up, that cost it around £15 million. A series of telecoms providers, including Deutsche Telekom, were also hacked by GCHQ. Those are law-abiding companies. They are not terrorists. They have information and are a conduit to further information, perhaps, but they are also people who can be compelled to co-operate with their own national authorities. However, GCHQ, under this warrantry and hacking regime, has instead taken the view that foreign, legitimate companies with international stature, within the bounds of Europe where we have common laws and systems, are a legitimate target for hacking, and that the clean-up operations are, frankly, not our concern.

Lord Butler of Brockwell: Could we stay within the UK for the moment?

Jim Killock: But this is a UK operation.

Lord Butler of Brockwell: I know that it is a UK operation. I am just talking about the targets at the moment. The point that you have made is about overseas targets. That is a separate consideration. Within the UK, you must agree that it is an advance that this proposed Bill gives specific authority for and introduces transparency into that power.

Shami Chakrabarti: I agree with that. I wou*l*d just like it to be more tightly regulated, given the consequences.

Lord Butler of Brockwell: Sure. You are not arguing, are you, that such a power, properly warranted—we have had discussions about what proper warranting is—may not be a legitimate weapon?

Shami Chakrabarti: In extremis. The intrusion is graver, because it is not just surveillance but actual damage—not least, potentially, damage to fair trials, if now every criminal defence lawyer can argue, "This isn't a genuine email. This isn't genuine data any more, because of hacking capacities". Given how serious the consequences of hacking are, the thresholds possibly need to be even higher than for other powers in the Bill.

The Chairman: I will now move to Lady Browning and Lord Henley. I am conscious that there is a vote in the Commons at 7 pm, but I would very much like the Commons members to be here for the questioning.

Q135 Baroness Browning: You have all expressed concern about Clause 189. I wonder whether you could share with us what you believe the effects will be on both service providers and customers. Ms Wilson Palow, your submission stated very clearly your concern about this.

Caroline Wilson Palow: It is a very broad power, to begin with. Essentially, it says that obligations can be placed on service providers to facilitate interception, hacking or any other power in the Bill, and they would need to take those steps ahead of time, before an authorisation or warrant was placed. Within that broad power, there are some examples of what might be done. A particular concern of ours is the removal of electronic protection. We interpret that as the potential to undermine encryption. Encryption is crucial to so much of what we do all the time, including all our financial transactions. It gives us the security to operate online. The removal of encryption has the potential to undermine all of that. We think that the balance there has not been struck appropriately.

Shami Chakrabarti: Taking my real-world analogy again, because of my poor understanding of these things, I do not think that it would be proportionate to give government the authority to demand that every locksmith in the country makes a spare key every time he is setting a lock for a home, a property or whatever. It is proportionate in certain circumstances, under warrantry, for the authorities—the police—to break into a targeted property because we believe that there are explosives, contraband or evidence there. To ban privacy, to ban private conversations and to require people who live on trust—companies that are all about creating a space of trust, so that we can have trust in our banking system et cetera—to leave those gaps in the nation's cybersecurity is quite problematic.

Renate Samson: It is the point that we were making earlier. The Bill is about protecting society. Encryption enables the protection of society. It enables people to use Crimestoppers. It enables whistleblowers to lay clear things that are going on that benefit society. It enables the vulnerable to communicate safely. Battered wives, for want of a worse expression, can ensure that they communicate as necessary. People on witness protection programmes can have an element of safety. It is much broader. It involves all of business. When all the communications in our home and everything else we have talked about on the Internet of things are connected online, we all want to know that our energy can be supplied safely. Encryption, as our submission to you explains, is not just a concern of privacy campaigners. It is a concern of Governments and business and one that will impact on us all, as all our lives are lived online.

The Chairman: Thank you very much. I move now to Lord Henley, on the Wilson doctrine and other matters.

Q136 Lord Henley: There is protection in the draft Bill for legally protected communications of journalists and journalists' sources, and there are protections for Members of Parliament of both Houses, enshrining the Wilson doctrine. Do you think that the Bill goes far enough?

Shami Chakrabarti: Not at all. There is room for some serious improvement. Let me be positive: there is room for real improvement. As far as I can tell, the Wilson doctrine has been completely reneged on. Recent statements by the Prime Minister suggest that, effectively, there is no Wilson doctrine in practice any more.

Lord Henley: What particular comments of the Prime Minister are you referring to?

Shami Chakrabarti: My understanding of recent statements from the Prime Minister is that there is now no absolute practice of not intercepting parliamentarians' communications. That was an absolute promise that came from Prime Minister Wilson and, indeed, was repeated by subsequent Prime Ministers.

Lord Butler of Brockwell: No. I am sorry, but you are wrong about that.

Shami Chakrabarti: I have read the Wilson statement. As regards what could be improved, I accept that there could be certain very rare circumstances where it would be justifiable, in a democracy, to interfere with even the communications of parliamentarians, lawyers and journalists, but we want something closer to the provisions that you currently have in place for production orders. You want something approaching reasonable grounds for believing that a very serious criminal offence is happening or has happened, and that there are no alternative ways of getting to the evidence; otherwise there are real dangers. Think of the political dangers. Perhaps it was just a rhetorical flourish, but we have had leaders of parties suggest that opposition parties are a threat to national security. I do not think that it is healthy for democracy for opposition political parties to believe that it is possible that they can be intercepted just on the say-so of a political opponent, even if that political opponent is the Prime Minister.

When it comes to legal professional privilege, we now know, because of the Belhaj case, that the security agencies were looking at legally privileged material that was relevant to a case being brought against them in relation to torture. There need to be much graver safeguards—we are back to judicial warrantry—and a very strong presumption against looking at parliamentarians' communications, legally privileged communications and journalists' sources.

The Chairman: Thank you very much. I will give you just one or two more minutes, because I want to wrap up with a couple of suggestions about how you can give us more evidence.

Jim Killock: I want to say something very specific about this. It is very hard to tell where the boundary between journalist and non-journalist lies. In this day and age, it is not somebody who is working on a paper; it could be somebody writing a blog and self-publishing. Many NGOs have a similar role to journalists in exposing, commenting and publishing. Particularly with communications data, where the system sometimes has to go to a magistrate or

whatever and sometimes has to be self-authorised within the police, it breaks down when you have this blurring, which is a very strong reason why all authorisation should be done by an independent authority. That, in particular, has been spelt out in the data retention judgment by the CJEU; when communications data are accessed—in that case, it was talking about retained data—there should be independent authorisation. This is one of the reasons why.

The Chairman: Thank you very much. It has been a fascinating session. It really has—very revealing. If in the evidence that you present to us you want to go into some of the detail of any amendments or drafting issues that you feel would improve the Bill, which you mentioned earlier, please feel free to do so and send those suggestions to us. Thank you very much for coming along today.

Mr Owen Paterson MP (QQ 94-100)

Evidence heard in public Questions 94-100

Oral Evidence

Taken before the Joint Committee

on Monday 7 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Bishop of Chester, Lord Henley, Lord Strasburger.

Witness: **Mr Owen Paterson MP**, gave evidence.

Q94 The Chairman: We give a warm welcome to our colleagues, Lord Blunkett and Mr Paterson. First, we apologise to you. It is largely the fault of the House of Commons; it decided to have a vote and that put the whole business on by about 15 minutes. We are extremely grateful to you both for coming along to talk to us about this very important Bill. Because of your experience in government, both of you know a great deal about the issues involved, so we are very grateful indeed. I will take advantage of my position as Chairman by asking the first question, which is for Lord Blunkett and for Mr Paterson. It is a very simple one. Is this Bill necessary, in your view?

Lord Blunkett: I cannot promise to be anything like as riveting as the last session, Chairman. Could I declare a non-pecuniary interest? I have an interest in a company that is involved in verification and authentication in the payments business, so I have a bit of knowledge—not as much as your previous contributors, obviously—about what will drive companies out of Britain.

Yes, the Bill is necessary. It required updating, for the reasons that I spelt out in my written and oral evidence to the ISC, and if people have insomnia they are very welcome to read it. I will not repeat all that, except to say that we have moved from an analogue to a digital age. For some time, we have needed to update the former telecommunications procedures and safeguards for the age we are in at the moment. My precept has always been that we use the same principles. When I hear people suggest that somehow there is an issue with holding telecommunications data long enough to be able to access it when necessary, or that it is the same as the content, I wonder whether they would have used the same arguments if we were discussing this 20 years ago, in the telecommunications age that existed then.

The Chairman: Thank you very much. Mr Paterson, is it necessary, in your view?

Mr Owen Paterson: Chairman, thank you very much for inviting me to your Committee. Yes, I think that broadly it is, to bring the powers that our agencies have up to technological speed with our opponents. Having worked in Northern Ireland, as you did, I have no doubt

of the real dangers posed to our citizens on a daily basis. It is only right that we give the incredibly brave people who work in our security agencies every necessary tool in order to beat them. I totally agree with Lord Blunkett. The original principles should always prevail in how we oversee and manage this intrusion.

Q95 The Chairman: Before I move on to colleagues so that they can ask about interception and authorisation, which both of you are very knowledgeable about, I have one more question. A lot of the Bill covers bulk interception, bulk acquisition of collection of communications data and bulk equipment interference. Do you think that an operational case has been made for that?

Lord Blunkett: The term "bulk"—people talk about metadata—provides a fog around the issue. Surely the fundamental issue is that what is taking place requires monitoring. If monitoring involves collection of data, where should those data be held? Six years ago, the Government backed off the idea that there should be any attempt to hold centrally, so we are asking the private sector to co-operate. We are doing so in a way that allows the agencies to be able to do the job. We need to demystify this, if I may say so, because the term "bulk" worries people. The fundamental issue, which was touched on in your previous session, is what in a practical sense can be undertaken, and what meaningful information can be gleaned from it for acceptable purposes. If we drill down to that, we start to demystify it and can then challenge the agencies as to whether what they are doing is relevant to the objective that we have laid out for them.

Mr Owen Paterson: I broadly agree. Once the principle of interference and capture of private data is accepted, I am not worried whether it is a small amount of data or whether it is a bulk amount of data—which, as Lord Blunkett said, has become a bit of a shibboleth. The principle must be that this data are managed in a responsible manner. In my experience, our services have been punctilious in the manner they respect the constraints and the protocols put on them.

Lord Strasburger: On the subject of bulk, is it not true to say that the concern is not necessarily about the quantity but about whose data are being captured? There is a difference between surveillance or interception of the data of suspected criminals or terrorists and surveillance or interception of those of the rest of us. It is targeted against untargeted, rather than bulk against small.

Lord Blunkett: We have always collected them. They have been collected, have they not? They have been held. The records have been there, under the old telecommunications system. They were not accessible in the same fashion as they are now, at the speed they are accessible. Collation is possible, with new technology addressing new technology, but the process was the same, was it not? The data was held.

Lord Strasburger: It was not quite the same. In the case of telephone data, the data was held by the telephone companies for their own billing purposes. In the case of Internet connection records, we are asking the ISPs to create the data, which do not currently exist.

Lord Blunkett: We need, perhaps, to ask the ISPs, as you are presumably doing, what they do with the data, because the idea that they hold them now only for billing purposes is mythical. The amount of data that is used by ISPs for all sorts of purposes—people seem

willing to provide and to collaborate with that—is enormous. Just ask how much a Sky box provides, if we consider what is done with it afterwards.

Mr Owen Paterson: We are broadly in agreement again. Huge amounts of data are kept on every one of us, every day. It is the manner in which those data are used—whether they are used responsibly and whether we have the right protocols to control that use of data—that worries me. That is the main concern.

Q96 Mr David Hanson: You have both exercised the authorisation of intercept warrants, in Northern Ireland and in the Home Office. Could you give the Committee a flavour of how urgent those requests were, how often you turned them down and whether there were any detailed issues—without referring to cases—that you think the Committee would wish to reflect on in relation to the existing authorisation procedure? Perhaps you would like to answer, Lord Blunkett. I can see Mr Paterson passing over to you.

Lord Blunkett: I am happy to do so; I was just trying to share the burden a little. Let us try not to exaggerate. Many of the warrants authorised—there are probably slightly more now than there were in my day, but there were about 2,500 a year—came through on a process of sensible authorisation, which gave time to look at the detail. They were often renewals of authorisation previously given, on a three-month basis, and then more frequently after that.

There were occasions when it was absolutely vital for the services to have an answer in the middle of the night. I am trying not to exaggerate it, because this is not about theatre—it is about reality. On more than one occasion when I had switched off my mobile phone and was not at home, I was literally dragged out of bed by the protection team. When you get one, you have to do it there and then, although in the middle of the night you are not as compos mentis as you might be and you question whether you should pause, drink a coffee and make sense of it. As a whole, it was necessary to be able to turn them around speedily. I know from the questions that Owen has raised in the Commons that both of us are concerned that on critical occasions an incident cannot occur because an authorisation has been delayed.

You asked me a second question: how often did I turn down requests? Out of the numbers we are talking about—I have thought about this a lot—I would say about 2% or 3%. Some of those then came back with further information and clarification that helped me to see that they were necessary.

Mr Owen Paterson: When I arrived at the Northern Ireland Office, it was quite a delicate period. Your Government had just got devolution of policing through. Sadly, there was an element of the republican community that was completely determined not to accept the settlement and wanted to continue physical violence and terrorist actions. They were extremely dangerous. Sadly, we had to ramp up our activity, to get quite a lot of extra money from the Government and to re-equip certain agencies.

I was very aware that we were fighting a 24-hour campaign. One of the first things that I did on day one was to make it very clear to my private office, “This is a priority for me. You wake me and interfere with what I am doing at any time. Never, ever, put my private convenience before speed in bringing one of these requests for a warrant to my attention”.

The vast majority were done in an orderly manner. We had diary slots once or twice a week; I cannot remember how many. As David said, they were frequently repeats. Sadly, it was the same old names coming round and round every three months. As David said, occasionally I would be woken up at 2 or 3 o'clock in the morning and asked for a very urgent decision. That is what has provoked me to make public comments that I am extremely concerned about some of the proposals in the Bill that might interfere with swift executive decision-making.

On the number that I turned down, I am with David. It was a very small number, but I did. It was known that I was not a patsy. I turned down the ones I was not satisfied with, or I sent them back for further information.

Mr David Hanson: That leads to two questions, which both of you can answer. First, how do you now feel about judicial oversight of that process? Is it fair, proportionate and the right thing to do? Secondly, given the concerns that Mr Paterson has raised publicly in the Commons, is there a definition for you of the turnaround time in an urgent case for any judicial oversight commissioner who may be appointed under the Bill?

Lord Blunkett: I am happy with the compromise—I suppose you would describe it as the sophistication—if the process of review is in tandem with the Secretary of State's decision-making process. Historically, judicial review is exactly what it is: a legal and administrative review of the way in which the Executive or their agencies use powers that have been granted to them. In our present process of commissioners, it is down the line when the process is reviewed and checked. This would mean that every decision would be subject to that tandem process. I would be unhappy with it if it cut out the Secretary of State, and those who are vehemently against any kind of intercept and surveillance measures would be horrified if there were not some sort of review now. We are trying to get that in tandem.

Mr David Hanson: It is more approval than review.

Lord Blunkett: That is the debate you are having—to clarify what it is. If it is not a review, are the commissioners being reviewed down the line? There is a presumption in our present political environment that judges know better than anyone else and are better than other people at all sorts of processes. I think that they are very good at interrogating and being able to make judgments in the critical judicial system that we have. I do not think that they are any better or worse than senior politicians at making a judgment on whether the evidence placed before them in these circumstances stands up. If I may be controversial, Chairman, because you have been through it yourself, sometimes you weigh the evidence and use instinct. Instinct is no less valid from those who have come through years and years of the political process and have been publicly scrutinised themselves than it is from judges.

Mr Owen Paterson: I would go further than David. I am wholly in favour of strengthening the review procedure after a decision has been made. Whenever I signed one of these things, I was fully conscious that I was subject to quite a rigorous inspection in the cold light of dawn, possibly some months later. I was fully conscious that I could be summoned to a Committee like this and could be hauled up on the Floor of the House of Commons in Questions. There was a real responsibility. However, I really believe that it is vital that the decision is made rapidly by a Secretary of State with full executive powers of decision-

making. It is up to the Secretary of State to make a decision, often under very imperfect conditions and with imperfect information. As David has just said, often you may have to trust instinct. Our current Home Secretary has done it for five years and is extraordinarily well-placed to make difficult decisions. I wholly fail to see the value of distinguished judges coming in and taking part in the decision. I really oppose it. Go back to Montesquieu and the separation of powers. Their skill is interpreting law or, here, interpreting the manner in which a law has been put into action by an Executive. I feel very strongly that these are executive decisions. They are operational decisions and must be made by a democratically elected Minister, accountable to Members of Parliament.

Mr David Hanson: This is the final question from me. The key element will be the interface between an urgent request to you as the Secretary of State for one or both departments versus a judge reviewing that decision and taking a different view on an urgent case. Where does responsibility lie in the event of that type of conflict?

Mr Owen Paterson: This is what worries me. I stressed in my opening comments that often a swift decision needs to be made. The Secretary of State will be very conscious of his or her responsibility and will make that decision. Here you have a second body party to the decision. Clause 138(3) states, "Where a Judicial Commissioner refuses to approve a decision to issue a warrant under section 137, the Judicial Commissioner must give the Secretary of State written reasons for the refusal"—written reasons. How will that work if the Secretary of State for Northern Ireland is in one place, the commissioners are in another and there is information that may have come from our allies in the Garda Siochána that an operation is under way?

The pass on this has partly been sold. There is the equivalent of an emergency provision, where the commissioners have five days to make a decision. Frankly, that could apply to everything. I would be happy with that. I am perfectly happy to have more judicial scrutiny, more frequent review and more regular meetings with the relevant Secretary of State. They came to see me probably once every six months; you could do that much more frequently. I am very strongly opposed to a member of the judiciary making a co-decision. That is really dangerous. What happens if it goes wrong? Who is to blame? Who comes before Parliament? Who do the relatives sue if a bomb has gone off and a Secretary of State had made a valid decision, under difficult circumstances, with imperfect information, but it had been skittled by a very well-meaning, very well-trained judge on a legal nicety? This has not been thought through. Do they get together in the middle of the night and look at the written review? Do they then together go back to the agency and ask for more information in the middle of the night?

It has not been thought through. I see delay and muddle. There has to be a difficult decision, made by an elected Minister, who is subject to intense scrutiny after the event. This muddles the role of the commissioners. If they are to be a serious body, reviewing and scrutinising, they are compromised if they are active in this decision. It will go one of two ways. Either they will become patsies, to use my earlier phrase, and will just go along with the Secretary of State, so they will be devalued, or they will become an extra body that is not accountable to Parliament. Either of those results is very unsatisfactory. To make it even worse—to get you depressed—it is much worse in Northern Ireland, where you have divisions among judicial bodies, as we saw with the Duffy case collapsing only last month.

Q97 Victoria Atkins: My question has been answered by both of you. The question is, who judges the judges under this format? Please correct me if I am wrong, but there is no accountability for the judicial commissioners, whereas the Home Secretary is accountable to the House of Commons and Select Committees in this place.

Mr Owen Paterson: As I said, I am very concerned that these judicial commissioners will not be accountable. Then there is a third human being with the powers of Solomon, according to the Bill, called the Investigatory Powers Commissioner. If you look at the same clause—Clause 138—subsection (4) states, "Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to issue a warrant, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant". That introduces a third body, with more muddle, more delay and more lack of accountability. I go back to my comments to David Hanson. What happens if it goes wrong? Who is to blame? Who is hauled up before this Committee? Who is hauled up before the Northern Ireland Affairs Committee for letting an operation that could have been stopped go ahead, when the democratically elected Secretary of State had made a clear decision? I am not at all relaxed about these proposals. I really do not like them.

Lord Blunkett: I share Owen Paterson's genuine concern, but I also know, with a political hat on—this is why your Committee has a massive challenge, but why it is sensible to have scrutiny of the Bill in this way—that we need to find a way of ensuring that a tandem process can work, simply because there is an atmosphere now, driven by those who suspect the state of all sorts of things, that makes it very difficult to resile from what has been put forward. Sophisticating it will be the challenge. I would like to wish you luck with that.

Dr Andrew Murrison: Answerability is an important concept, but what does it mean in practice, since Secretaries of State answering on warrantry issues will invariably say, "We do not comment on security matters"? The other point, just for observation, would be the stance taken by the rest of the "Five Eyes" community in relation to judicial oversight, which, even under the Bill as it is currently drafted, is quite different. Do you think that there may be scope for separating warrantry on criminal matters from warrantry on national security matters, removing the Home Secretary from the former?

Lord Blunkett: The problem we have had with authorisation is that the more dangerous the individual or individuals, the more likely it has been that the Secretary of State—or, in the case of criminal behaviour, the Home Secretary—has been dealing with it. We have had almost a perverse situation where the police—obviously you will look at this separately, but I said it in my evidence to the ISC—have been able to get authorisation to do things without going to the Secretary of State. I think that we have it the wrong way round. The Secretary of State should be responsible for the warrantry, for the reasons you are very familiar with. You cannot separate serious crime and the danger of terrorism, not least with interconnection, money laundering and everything that you were debating before we came in.

Dr Andrew Murrison: Would it be a little easier if we had a proper definition of national security, which we do not have on the face of the Bill at the moment?

Lord Blunkett: We have all sorts of articles in relation to exemptions, do we not, within the European Union—I dare not mention it in Owen Paterson's presence—as regards definitions? Earlier Sir David Omand indicated that we have got as near to it as possible, in an imperfect world.

Mr Owen Paterson: Could I add one or two comments? First, I do not entirely agree that Secretaries of State just bat off these questions and say, "It is not appropriate to reply". When serious incidents happen, often there are quite major investigations and what went wrong comes out. This will happen only when something goes horribly wrong, so the process will be exposed.

On the issue of criminal or terrorist issues, I totally agree with David Blunkett. In Northern Ireland, where you cross the line between excessive fuel smuggling, racketeering and drug smuggling feeding violence, which may be criminal or terrorist violence, it is a pretty grey, woolly area. Both those came across my desk, and I did not differentiate.

Q98 **Suella Fernandes:** I have two small questions. You have talked about the notion of instinct that Ministers may have when issuing warrants that the judiciary may not possess and said that it is an important factor to preserve in the decision-making process. Could you say a bit more about what distinguishes the ministerial perspective on such decisions from a judicial approach?

Lord Blunkett: The judicial approach would obviously get there, because after time they would be familiar with the process. That happens to Secretaries of State coming in, but on the whole you do not get people who are inexperienced in the general areas who are Home Secretaries, Foreign Secretaries and Secretaries of State for Northern Ireland. They are still learning when they come in and when they are doing it, as we all are when growing into jobs. I am sure that, after a period of time, those who have been schooled and have undertaken their process of promotion in an entirely different way would come to expect to have to use instinct, but it is not helpful to a judge to use instinct, is it? Judges are not trained to use instinct. They are trained to resist using instinct, are they not, at least theoretically? The facts have to be dealt with, even if the judge believes there is a problem. All I am saying—I am trying to be honest about it—is that you examine the material that has been put before you and do everything that you can to stick to that, rather than what you feel about it, but there are occasions when you think, "I will go with it. My instincts tell me that there is something entirely right about the application and entirely wrong about what these people have been doing".

Suella Fernandes: Would you say that it is a wider perspective, as opposed to a narrower legal perspective?

Lord Blunkett: Inevitably, yes. If it was only a legal matter, you would not have that process at all.

Mr Owen Paterson: That is exactly right. If this was nice, rinky-dinky, clean and tidy, you would not need politicians. You would have these wonderful judges who were all knowing and all knowledgeable, who interpreted law that told them exactly what to do and who did not move an inch off it. If you look at Clause 169(5) and (6), they are expected to make

political judgments. It says, “In exercising functions under this Act, a Judicial Commissioner must not act in a way which is contrary to the public interest or prejudicial to—(a) national security, (b) the prevention or detection of serious crime, or (c) the economic well-being of the United Kingdom”. The judicial commissioner must ensure that he does not “jeopardise the success of an intelligence or security operation or a law enforcement operation … compromise the safety or security of those involved, or … unduly impede the operational effectiveness of an intelligence service, a police force, a government department or Her Majesty’s forces”. Every one of those requires a difficult political decision. There might have been information from Dublin that someone is on the way up. Someone else is coming in from Donegal. You do not have perfect information. You have to trust the information you have been given and you have to make a subjective judgment. You are fully conscious that you might be up for very severe scrutiny—in my case, some months afterwards—in the cold light of day, and you have to make a decision. There is nothing clean, rinky-dinky, nice and tidy that can be delivered to make it easy for a judge. It is absolutely what judges are not trained to do, as David said. It is exactly the opposite.

I am very happy with the five days. I would be very happy with five-day scrutiny and with the Secretary of State being called in every month to meet the commissioner, who would say, “You made this, that or the other decision”, and go over it, but at the critical moment, at 2 or 3 o’clock in the morning, somebody has to make a very difficult decision, and it may be on instinct. In my case, I had been going to Northern Ireland every single week as the Opposition spokesman—as the shadow Secretary—for three years. I had met an awful lot of people, I had been to every corner of Northern Ireland—places where, sadly, I could not even dream of going now—and, in fairness, I learnt a little bit about it. I pulled on that information and on some of the people I had met. David is absolutely right. There is an element of this that is instinct. That is called political judgment. It is not right to put judges in the same box. It is not fair to them.

Suella Fernandes: Where would you draw the line, in striking a balance between national security and transparency in decisions on the issuing of warrants, between judicial and ministerial decision-making power? Would you say that it should be solely for Ministers, with no judicial decision-making power?

Mr Owen Paterson: Yes. I am completely clear. Elected Secretaries of State, accountable to the House of Commons, should make those difficult operational decisions. That will guarantee operational agility and swift reaction. I am all for increasing, extending and making more intense the scrutiny process by distinguished judges, after the event. I mentioned dear old Montesquieu and the separation of powers. It is not a bad thing to go on. He made it absolutely clear that you do not have judges making executive decisions.

Q99 **Bishop of Chester:** The clauses to which you referred are in Part 5 of the Bill, I think, at the end, on bulk interception warrants.

Mr Owen Paterson: Part 8.

Bishop of Chester: Earlier warrants allow a five-day period when urgent decisions can be taken. Is there a particular reason why you think there should be the facility for an urgent decision, not requiring the judicial approval in the later part you have been referring to?

Mr Owen Paterson: I am very happy with the five days. That could be a sensible compromise. The five days allow decision-making by the elected Secretary of State, without interference, without delay, without obfuscation and without muddle.

The Chairman: Can I stop you for a second to clear things up? The five days refer to urgent cases, not ordinary cases. I think that Mr Paterson is saying that, even in ordinary cases, the five days would become a review, rather than a co-decision.

Mr Owen Paterson: Correct. That is exactly right.

Bishop of Chester: There is the practical question of an urgent request, under the later part of the Bill, for the bulk warrants, but there is not provision for an urgent decision. There is in the earlier part of the Bill. You are raising a more fundamental principle as to whether the judges should not operate as they do now, revealing after the event. You are suggesting that that is much better.

Mr Owen Paterson: The Chairman summarised very effectively what I think. The decision should be made by a democratically elected Minister, accountable to the House of Commons. The review should be conducted by distinguished lawyers, days, if necessary, after the event, with the scrutiny process starting at five days. I would be very happy for Secretaries of State to meet the reviewers more regularly.

Bishop of Chester: I understand that that is how DRIPA, the present time-limited Act, operates. There is judicial review after the event.

Mr Owen Paterson: Yes.

Bishop of Chester: That is what you would prefer.

Mr Owen Paterson: There is no judicial co-decision-making. At the moment, judges do not participate in the decision. Under these proposals—it is called the double lock in all the press releases—they will be very actively involved.

Bishop of Chester: To be quite clear, you are striking, in a sense, at the heart of the principle of what is now proposed.

Mr Owen Paterson: Yes. I strongly disapprove of the proposal that judges make executive decisions.

Bishop of Chester: That is what you are saying.

Mr Owen Paterson: Correct; absolutely.

Lord Strasburger: Could you tell us how many times you were held to account by Parliament? Could you also explain why your views, in particular, are the exact opposite of those of our four “Five Eyes” partners?

Mr Owen Paterson: I do not remember ever being called up before any Committee or having it raised in questions in Parliament. I suppose you could say that that is a tribute to the fact that the system works, in that people were careful before putting requests before

me and, I hope, I was also careful in scrupulously reading every detail and not nodding things through. As I said, I did, infrequently, turn them down.

Lord Blunkett: Let us go back. The commissioners reviewed the process and whether we had followed it, within the powers laid down to us, which is what I understand review to be anyway. We also had the annual debate, which, sadly, did not engage the media in the way I had hoped it would. Parliament usually had a robust debate, concentrated mainly not on Northern Ireland but on the Home Office and the Foreign Office, with some thoughtful contributions, but it was not really holding to account in the sense of people understanding and then asking us to explain what we had done in individual cases, for fairly obvious reasons—we were dealing with sensitive material, which we would not be able to explain. That was one of the Catch-22s about reporting back to Parliament when we were debating Bills, including the one that has a sunset clause next year. How can you report to Parliament on detail that is itself subject to the necessary privacy that protects those who have been involved? That is why your job, and the Home Secretary's job, is so difficult.

I fall slightly short of Owen's absolutism on this. I can see entirely where he is coming from, but in the reality of the moment we have to deal with what has been put forward by the Government and the difficulties that they face. I have to be careful here. My second son works for a major company and years ago used to tell me off for being too gung-ho on all this, so I have family problems. Can I be clear? Whatever the Government decide to do, there are people who do not believe that it is either necessary or acceptable. At the moment, they get a bigger hearing than the intelligence agencies.

The Chairman: Could I clarify something Lord Strasburger said? He made an important point. There is no real parliamentary mechanism currently available, is there, for obvious reasons, that could in any way scrutinise the decisions either of you would make on agreeing intercept warrants—even to the extent, I guess, that the ISC, meeting in private, would not be able to deal with them?

Lord Blunkett: I see no reason why we should not have a much more thoroughgoing report on the number of decisions taken and the nature of those decisions. When the then Foreign Secretary, William Hague, reported to Parliament on the back of what happened with Snowden, I said that we could be a lot less diffident and sheepish about all this, without putting the intelligence and security services and their operatives at risk. We should examine how we might do it more openly. We could also examine areas that are outwith what the Bill is able to deliver, namely where information is provided from other agencies outside this country and there has been no warrant and no clearance. The information is given to us, and we have still not come to terms with that.

Lord Strasburger: You seem to be confirming the view that the concept of parliamentary scrutiny of warrants is a myth.

Lord Blunkett: I do not know anyone who has really believed that Parliament scrutinises the warrants system.

Lord Strasburger: Exactly.

Lord Blunkett: The commissioners have. They produce their annual reports, which are usually commented on in the media, but Parliament, other than in the annual debate, does not and has not.

Lord Strasburger: But both of you gentlemen, particularly Mr Paterson, have waxed lyrical about the concept of parliamentary scrutiny. I am struggling to see where it is.

Lord Blunkett: No. The politician is accountable. That is different from the way in which Parliament chooses to scrutinise or not to scrutinise. Secretaries of State are accountable, both publicly and to Parliament, and can be sacked. I wonder under what conditions a judiciary involvement would result in their being removed.

Mr Owen Paterson: That is the key point: we are accountable. There is a lot of information about decisions made by Secretaries of State. Ultimately, those decisions can be taken up by parliamentarians, should they choose to do so. As David said, at the moment there is only a debate. Should things go wrong, Secretaries of State can absolutely be on the line and accountable to Parliament.

Lord Strasburger: As far as I know, it is not legal for a Secretary of State to discuss a warrant in public.

Mr Owen Paterson: But a Secretary of State is accountable to Parliament for activities in his or her sphere of influence—and can be fired.

Victoria Atkins: I can help Lord Strasburger. Sections 17 to 19 of RIPA make it a criminal offence for Secretaries of State to answer questions on this, if they are so asked. That may help to answer his question.

The Chairman: You have been let off the hook today.

Lord Blunkett: That never passed across my consciousness when I was there.

The Chairman: I move now to Lord Henley, because Mr Warman's questions have been answered.

Q100 Lord Henley: I want to come on to the various safeguards for privileged communications. You will remember the statement that was made by the Home Secretary on 4 November and the concerns raised by David Davis, in particular, about the lack of protection that MPs have over the potential acquisition of their communications data. Does the enshrining of the Wilson doctrine in statute provide adequate protection for legislators' communications and address the concerns put forward by David Davis, or should there be additional safeguards over the use of communications data for parliamentarians, as there are for journalists?

Lord Blunkett: It may be worth cross-referencing briefly to the inquiry that took place after the incursion into the Palace of Westminster in the Damian Green affair. That was old-fashioned taking away of materials, as opposed to intercepting them through new, modern information, communications and Internet provisions, but the principles were the same. That Committee, on which I served, was under the chairmanship of Ming Campbell, now

Lord Campbell. It is worth testing it out. If we are honest about it, the Wilson doctrine was more in intention than it was in reality. How carefully can I put this? What you are doing in this improved Bill is what we were trying to do. My predecessor, Jack Straw, brought in RIPA, and I had the undoubted "privilege" of implementing it. The intention was to be helpful, although people have interpreted it entirely differently since. On the Wilson doctrine, we should distinguish what is privilege in terms of protecting Owen Paterson's electors—my previous electors—from the issue of protecting the parliamentarian. Over to you, Owen.

Mr Owen Paterson: That is a good way of putting it. The principle of privilege, not the individual, is the key point. My main concerns with the Bill are to do with warrantry and powers of decision-making. When it came out, I read it and saw the statement that any proposal involving an MP or any other elected body—the Scottish Parliament, Welsh Assembly et cetera—has to go to the Prime Minister. There has to be an element of common sense. To go back to Suella Fernandes's question, it is a bit of instinct; anyone who thinks of putting any marker down on an MP has to think really carefully in advance. Common sense will probably be the best defence.

The Chairman: That was another very interesting, riveting session. We are very grateful to you both, because it has come from a totally different perspective from that of our earlier witnesses and gives another interesting aspect to our deliberations. No one can say that both of you have not put your views with great robustness. Thank you very much for coming along

Professor Christopher Forsyth, Policy Exchange (QQ 216-223)

Evidence heard in public Questions 216-223

Oral Evidence

Taken before the Joint Committee

on Monday 21 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Suella Fernandes MP, David Hanson MP, Shabana Mahmood MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Lord Hart of Chilton, and Lord Strasburger.

Witness: **Professor Christopher Forsyth**, Policy Exchange, gave evidence.

Q216 The Chairman: A very warm welcome to you both. Thank you so much for coming along this close to Christmas. We very much look forward to hearing your views on this extremely important Bill that Parliament is now considering. Apologies, too, for running a little late. I hope that it has not disturbed you. I will ask the first question, which will give you an opportunity to give the Committee your initial thoughts on the Bill. Do you think that it strikes the right balance between privacy and security? If it does not, how could it be improved? Should any other powers be included? It is really a very general question about your views on the Bill.

Robin Simcox: Many thanks for the invitation to speak here today. It does broadly strike the right balance. I might be in a minority of some of the people you have heard from so far in that I did not think that RIPA was an entirely unworkable disaster, but I appreciate that some clarity was needed with regard to bulk collection, which the Bill provides. It is also very useful for putting the powers in one place, one piece of legislation. The one thing that I might add as a word of caution is that the balance is right as the Bill is currently drafted, but I would be somewhat concerned if, during fierce negotiations in Parliament, it got watered down significantly on things such as bulk collection and the internet connection records. Those are quite fundamental powers needed by law enforcement and the intelligence agencies. The Bill is a successful piece of legislation that strikes the right balance at present, but I add that caution about losing any further powers contained in it.

Professor Christopher Forsyth: Lord Chairman, I am not an expert in surveillance, interception or security, so in a way my view on these matters is simply that of an ordinary citizen rather than an expert. I am afraid that, given the times we live in, it is inevitable that greater weight will be given to security over privacy in the balancing process than might otherwise have been the case, or even tolerable, in more placid times. To that extent, I recognise that the Bill provides for significant inroads on privacy, but it seems to me as an ordinary citizen, not an expert, that those inroads are justified.

The Chairman: Thank you both. That is very clear and concise.

Q217 Lord Hart of Chilton: We have heard in our evidence sessions a great deal about three interrelated subjects. I have three questions that I will put together. What is your view of the proposed double lock for authorisation of certain warrants? What is your understanding of judicial review principles? What is the correct balance between the respective roles of Ministers and judicial commissioners in the authorisation of warrants? Before you answer, I put to you an answer that Shami Chakrabarti gave at an evidence session here on 9 December. She said, "A double lock would mean, 'I can substitute my decision on the merits for yours'. Traditional judicial review means, 'I look at the way you made your decision, but I do not substitute my own for yours'. You have to be procedurally irregular or to have made a completely insane decision that no Secretary of State could make". I just wonder, since I know that you have written a paper on the question of judges taking the law unto themselves, what you think. First, is it a true double lock? Then, what do you understand the judicial review principles to mean?

Professor Christopher Forsyth: I will start with the judicial review principles, which used to be quite straightforward but are much less so now than they were. In 1984, in the GCHQ case, Lord Diplock said that there were three grounds of judicial review: procedural irregularity; illegality; and irrationality. The picture that he presents of judicial review is a situation in which you identify any one of those three grounds. If any one of those grounds is identified then the decision is open to be quashed. Outside those areas, where no ground has been established, the decision-maker—in our context, the Minister deciding whether to authorise a warrant—would be free to decide as they judged best in particular circumstances. There was a considerable degree of decision-makers' autonomy.

In his famous dictum where he set all this out, Lord Diplock also looked forward to a time in which proportionality might become part of the grounds for judicial review. So it has proved, whether it comes about through common law or through the effect of the Human Rights Act, that proportionality has assumed centre stage. This has had the disadvantage—some people would say the advantage—of making the process much more uncertain than it would otherwise have been. No one can be against proportionality in one sense—after all, we are all against taking a sledgehammer to crack a nut—but it is very easy to describe proportionality at the level of a slogan of a more abstract having the means and ends in balance. It is very easy to have that sort of description, but in reality it means a great deal of uncertainty. It is a very bold person who can predict the outcome of the decision-making process once proportionality enters the field. The principles of judicial review have become a much less certain concept than they would have been 30 years ago.

There is another consideration here that suggest that judicial review principles are, in a way, unsuitable or would have to be thought about a bit more carefully. I mentioned the three grounds of procedural irregularity, irrationality and illegality. Procedural irregularity is, of course, the principle that people should be heard and given the opportunity to make their case before a decision adverse to their interests is taken. That, of course, cannot happen in the kind of context that we are talking about—the interception of communications. It means that a whole slice of judicial review principles has been discarded for the purposes of this exercise. The effect of that would primarily be that the judges or judicial commissioners would tend to look more intensively to scrutinise more anxiously the decision-making process to make up for the fact that one is not hearing what

the person adversely affected—whose communications will be intercepted—thinks about this. Is that enough food for thought?

Lord Butler of Brockwell: Can I just ask a supplementary? Would the Bill be better without Clause 19(2), about applying "the same principles as would be applied by a court on an application for judicial review"?

Professor Christopher Forsyth: That depends on what you want to achieve by the Bill.

Lord Butler of Brockwell: Would it give more effective judicial control if that clause was removed?

Professor Christopher Forsyth: I suspect that if one was to strike out that clause you would end up with more effective judicial control. In fact, there would be a real danger of judicial duplication of what the Secretary of State decides.

Lord Strasburger: Would you call that a double lock?

Professor Christopher Forsyth: One might very well call it a double lock.

Lord Hart of Chilton: So on that basis the judge would be able to supplant the Home Secretary's decision with his own?

Professor Christopher Forsyth: I suspect that would be the outcome if you were to excise the subsection on judicial review. In my view that would be a retrograde step, although it would be open to Parliament to do it if it wished to. The Secretary of State ought to be making decisions on grounds different from those of the judicial commissioner. The judicial commissioner should make up his mind and assess the legality of the process, whereas the Secretary of State must surely show that she has acted lawfully but will take many other considerations into account. For example, if you were to intercept the communications of a foreign dignitary or diplomat there might be all kinds of consequences to that decision that it is right for the Secretary of State to take into account, but it seems to me inappropriate for a judge to take into account. But if that is what you want—the same criteria being applied to both elements of that decision-making process by the judge and Secretary of State—then so be it, but what are you achieving by the double lock if they are essentially deciding the same grounds?

Q218 Suella Fernandes: I should declare an interest that I was a student of Professor Forsyth's many years ago—you probably do not remember; I was a face in a crowd. Where do you think the line should be drawn between judicial and executive decision-making power in the context of warrantry?

Professor Christopher Forsyth: As far as common or garden serious crime is concerned, it has long been the case that these decisions—to issue a search warrant, for example—are taken by a purely judicial and not an administrative process. That is absolutely right. It does not seem necessary to me to have the Secretary of State's involvement in warrantry extending to the investigation of serious or organised crime. But when one is talking about national security or economic well-being, it is appropriate that the Secretary of State should take these wider considerations into account, which are inappropriate for the judge to take

into account. That is where I would draw the line. Of course, in all these areas, half-covered by secrecy or sometimes fully covered by secrecy, it is very difficult to lay down a principled position, but that would be my position. I am sorry that I do not remember you attending my lectures. I hope you benefited from them.

Suella Fernandes: I did, yes. Would you say that judges should not be involved in the issuing of warrants when it comes to national security matters?

Professor Christopher Forsyth: The Bill as it stands is a reasonable compromise in that judges can go into necessity and proportionality but they are to do so according to the principles of judicial review. If they do so according to the principles of judicial review—which means in this context that they will intervene only if they discover some ground for judicial review or a legal flaw in the decision—that seems right.

Q219 **Dr Andrew Murrison:** Professor Forsyth, how would you distinguish national security from serious crime? You appear to be suggesting that we should treat the two separately for the purposes of the powers discussed in the Bill. My second question is: should we not seek some sort of confluence with the rest of the Five Eyes community in the way that we determine warrantry and the various other powers in the Bill?

Professor Christopher Forsyth: Clearly, there will be cases where national security and serious crime overlap; for example, an organised money-laundering scam raising money for use in terrorist attacks or something of that kind. This is a definitional problem. Once national security became involved, I would think that it would trump ordinary serious crime and you would apply the national security criteria. But I recognise that that is a question of definition. On your question about seeking some sort of congruence with the Five Eyes community, that is so far beyond my understanding and experience—I know that the Five Eyes exist; I know very little more about them. It is clearly in the public interest that there should be close co-ordination among the Five Eyes. Whether that is achieved is above my pay grade.

Dr Andrew Murrison: I wonder if the Henry Jackson Society has a view, given its provenance.

Robin Simcox: Speaking for myself, close co-operation between the Five Eyes in this area is important but if you look at the issues to do with extraterritorial jurisdiction, what we need goes beyond the Five Eyes. If it was possible, there would be some kind of international treaty governing some of these areas because some of the things that DRIPA and the draft IP Bill look to do—for example, serving warrants against CSPs, making requests for data that are lawful in the UK but may contravene American law if those CSPs are based in the US—is where we are constantly running into the problem of overlapping jurisdictions and if there can be some progress made, as distant and unrealistic as that currently seems, considering some of the other countries that are involved in this, on an international treaty governing these things, that has to be something that we look at, to go beyond even the Five Eyes.

Q220 **Matt Warman:** We heard in the previous session about bulk interception being one of the most controversial issues. This always comes back to whether an operational case has been made for this sort of invasion of privacy. In your opening answers, you both indicated

that you thought that it had. Can you elaborate a little more on the operational case that you see has been made?

Robin Simcox: I think it has; it has to me, certainly. One thing that the UK Government have tended to do, as opposed to the US Government, who have sometimes not been as completely savvy on this as they could have been, is provide some of the real-life case studies of where this has been useful. The Government did this even in the draft Communications Data Bill back in 2012. David Anderson provided some examples and in the guide to the IP Bill further examples are provided. This is not just about terrorism; it is about fraud, other serious crime, stopping child exploitation, drug trafficking, et cetera. Providing those real-life examples resonates; it is too abstract without them. But I would also take it beyond that and say that the debate should be less about capacity and more about the strength of the oversight. It has been put to me in the past that, for example, we are relaxed about the Army having sophisticated weaponry because we trust the culture; we trust the oversight and that it will not be used against the population. You can apply a similar paradigm to our interception capacities. Having world-class intelligence-gathering is not a bad thing; it needs to be accompanied by extremely strong and responsible oversight.

Professor Christopher Forsyth: I agree. From my reading of the Bill and the associated documents, the case seems to be made for the necessity of bulk warrants to be granted in appropriate circumstances and the safeguards built into the Bill seem pretty considerable to me.

Q221 **Lord Butler of Brockwell:** Do you think that the draft Bill provides sufficient protection for legal privilege? It was put to us last week that there could be an absolute protection for legal privilege on the grounds that if a lawyer was involved in misdoing, that would remove legal privilege by itself because it would be a form of inequity. If you had a crooked lawyer, you could have legal privilege enshrined in the Bill but that would not stop the authorities intruding upon them.

Professor Christopher Forsyth: It is true that if the lawyer is found guilty of misconduct, he would not be able to rely on privilege. The difficulty is that the lawyer may be guilty of misconduct but you may not be able to prove it; you only suspect it. Again, I think the Bill has got it about right. I have no difficulty with that.

Lord Butler of Brockwell: Thank you. Did you want to add to that?

Robin Simcox: On the legal privilege side of things, I welcome the role of the judicial commissioner on this because there have been examples of the misuse of RIPA in the past, Andrew Mitchell and Plebgate being a very prominent example. But we cannot rely just on the role of the judicial commissioner here. There have to be properly trained single points of contact. Again, it goes back to the culture of the institution—the TS Eliot line about "dreaming up systems so perfect that no one needs to be good". There also needs to be a culture where powers are not wilfully and clearly misused, as seems to be the case on an isolated number of occasions with regard to RIPA and journalistic sources. So I welcome the role of the judicial commissioner but there needs to be a change in the culture as well, it seems.

Lord Butler of Brockwell: Yes, so with the role of the judicial commissioner, you think there is sufficient protection both for legal privilege and for journalists. Am I right in interpreting you both in that respect? Okay, thank you.

What about MPs? The protection there is the Secretary of State, the judicial commissioner and the Prime Minister. Is that sufficient protection for Members of Parliament, bearing in mind that the Prime Minister may be of an opposite political persuasion from the MP in question?

Professor Christopher Forsyth: The crucial safeguard there is the judicial commissioner. I do not think that giving statutory form to the Wilson doctrine would change very much, because it is difficult to see how that statute would ever be justiciable, other than perhaps providing a clearer audit trail when one of these decisions is made. One quite understands that individual MPs of one party might not believe that the Prime Minister is much of a safeguard when he belongs to a directly opposed party, but that is what the judicial commissioner is there to do: to see that there is no skulduggery in the approval of the warrant. If the judicial commissioner refuses, it is not going to get to the Prime Minister.

Lord Butler of Brockwell: Mr Simcox?

Robin Simcox: I have nothing further to add to that.

Lord Butler of Brockwell: Would there not be some advantage in putting the Wilson doctrine in law in the sense that if it is known that in due course at the appropriate time it has to be reported to Parliament that a Member of Parliament has been intercepted, this would make the Secretary of State more wary of doing it in unnecessary cases?

Professor Christopher Forsyth: I agree. That is what I mean by there being an audit trail, but I just do not see Clause 22 actually being litigated under in the judicial review court, so it would have no legal effect.

Q222 Suella Fernandes: I have a follow-up question on the issue that Professor Forsyth raised about judges and Ministers. There has been talk in our evidence sessions about the accountability and transparency of Ministers versus judges. Lord Carlile, who was the independent reviewer of terrorism legislation, has cautioned against the involvement of judges because of the lack of transparency, electability or accountability compared with Ministers. Could you comment on the comparison between the two arms and the importance of that in this context?

Professor Christopher Forsyth: I would echo what Lord Carlile says there. I recognise that there is a very strong political drive towards having the judiciary involved in this process, but the judiciary are not accountable in the way the Executive and Ministers are. Forgive me for putting it quite as starkly as this, but one would hate to see, after there had been some sort of dreadful outrage and the death of innocents, the Home Secretary facing an angry House of Commons and saying, "Well, I authorised a warrant to intercept these communications to find out what these wrongdoers were up to, but the judge refused it", bringing judges into the maelstrom of a political dispute. That it is putting it starkly, but that is the point about accountability: that given the nature of these powers, there needs

to be proper accountability, and the Executive and Ministers are accountable in a way in which judges are not.

Suella Fernandes: In what way? Could you elaborate?

Professor Christopher Forsyth: Ministers are accountable in that they will come before the House of Commons and Committees of this kind and have to justify themselves and answer difficult questions. The judges are not going to do that.

Suella Fernandes: I want to move on to another issue, overseas examples, and ask both of you whether there are any other countries that we could look to for guidance that have grappled with this issue.

Robin Simcox: This partially goes back to your previous question, too. The involvement of some democracies where the system and role of the judiciary are comparable to that of the UK—Australia, Canada, France and Germany—is significantly less than that of the UK. So there is that overseas example. The example of New Zealand, where the inspector-general of intelligence and security need not be a former judge, is sometimes cited, but I do not think you need to look to New Zealand to see how that can work well. Someone just mentioned Lord Carlile and David Anderson, neither of whom were sitting judges but both of whom were excellent lawyers who did a terrific job in the independent reviewer chair. Both have publicly done a great job in explaining that role to the public. They go on the radio and television and explain the role, and are an excellent link between the legislation and the general public's understanding of it. In this area we may decide that it needs to be a sitting judge, but the Carlile and Anderson examples provide a useful model for us here.

Dr Andrew Murrison: How do you feel that the idea of ministerial accountability in the areas we are discussing today can be lifted from the purely theoretical, since invariably when Ministers are asked about security matters in the Commons they will reply that it is not custom and practice for Ministers to comment on security matters?

Professor Christopher Forsyth: I do not think they are quite as reticent as that when they come before a Committee in private such as the intelligence services Committee. Is that not where their accountability comes through?

Dr Andrew Murrison: It is not very transparent, and I wonder whether you think that there are ways in which their decision-making can be made more transparent in real time. Of course, accountability can come to pass many years down the track, but that is of little help in the here and now.

Professor Christopher Forsyth: I think it is inherent within the intelligence services that things have to be kept secret that in an ideal world would not be kept secret, so I have difficulty in seeing how there would be accountability in real time. One can imagine that after a particular outrage and disruption and the death of civilian innocents the Home Secretary would come to the House and explain what was being done to track down the wrongdoers and to do whatever could be done to assist the victims, but would be extremely reluctant to provide any clear operational information about operations that might still be ongoing.

Lord Strasburger: But it is illegal for a Minister to discuss a warrant in public.

Professor Christopher Forsyth: I am not sure that that is the case.

Lord Butler of Brockwell: It is the case.

Dr Andrew Murrison: Do you think there may be grounds for reviewing that, given the double lock, which of course is different from practice in other countries with which we can reasonably be compared?

Professor Christopher Forsyth: Yes. I am surprised by that, quite frankly, but I think there would be occasions on which you would expect the Minister to be able to deal with the individual case, and that might allow them to discuss the warrant. So, yes, I think that should be changed.

The Chairman: Last but by no means least, Baroness Browning.

Q223 **Baroness Browning:** Thank you. I think Mr Simcox answered in reply to Ms Fernandes what I was going to ask, but I just wonder, Professor Forsyth, whether we could hear your views on the issue of the office of the Investigatory Powers Commissioner being led by a commissioner who has held a senior judicial position—at least as high as a High Court judge? What is your view of alternative models, such as the one used in New Zealand? I know that we have heard about other examples, but would you let us have your views?

Professor Christopher Forsyth: As I said earlier, I am cautious about the use of judges in this area. I recognise that there is a political need and a political demand for judicial involvement, but because of that general approach I see nothing wrong in principle with your inspector-general being a non-judge, as in New Zealand. If you look at some of the things that the New Zealand inspector-general has been doing, she has been acting in an entirely proper way in holding the services to account but in a way in which a judge might act. I think there are potential advantages to not having a judge, who inevitably is tied by the detail of the evidence, moving slowly and so forth. These are aspects of the judicial character. It may be good to have a non-judge dealing with these situations.

I would agree, too, that we have such good examples here of both Lord Carlile and David Anderson QC—non-judges carrying out these different legal tasks and doing so, if I may say so, with considerable success and very impressively. So I do not think that the inspector-general need necessarily be a judge, but it seems to me that very often the decision to involve the judges has been taken essentially for reasons of trust, because the other branches of government are not trusted sufficiently, whereas judges are trusted. I am not sure that that is entirely correct. When one looks at these things, as far as one can tell, not being privy to any secret information, these matters are dealt with very conscientiously and according to law entirely within the Executive at the moment.

The Chairman: Thank you both very much indeed. It has been a fascinating session. We wish you both a very happy Christmas.

Caroline Wilson Palow, Legal Officer, Privacy International (QQ 127-136)

Evidence heard in public Questions 127-136

Oral Evidence

Taken before the Joint Committee

on Wednesday 9 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Lord Henley, Lord Strasburger.

Witness: **Caroline Wilson Palow**, Legal Officer, Privacy International, gave evidence.

Q127 The Chairman: A very good afternoon to you—or evening, now. I am sorry that we are a little late—there was a vote in the Commons earlier. You are very welcome. I will make two points before I ask the first couple of questions. My colleagues will come in after that. Each of you has given your response to the Bill very publicly over the last number of weeks. The Committee has all the statements that you have made. In addition, of course, I am sure that you will give us written evidence. This is a very big Bill. It is very lengthy and very technical. Has subsequent analysis of the draft Bill led any of you to alter any of your positions from those that were taken in your initial response to the Bill's publication?

Shami Chakrabarti: I would simply say that I am possibly more alarmed by the Bill than I was at first glance. The Committee will appreciate that it is a long Bill.

The Chairman: Very long.

Shami Chakrabarti: It is very complex. Like all legislation, it requires an understanding of what its clauses actually provide, as opposed to how its clauses have been pre-briefed or spun in the press. It also requires a level of understanding of the relevant technology. Those two things have to come together. My own organisation is a human rights organisation with, traditionally, considerable expertise in legislation, but recent weeks have given us the opportunity to work with partner organisations that have a considerable level of expertise in the technical sphere. That experience makes me more alarmed now about the personal and cybersecurity implications of the provisions, however laudable and well-meaning they may be in their motivation.

The Chairman: Do your colleagues share that view? Are you more alarmed now, as the weeks go by?

Renate Samson: Initially I was very clear that there was a lot to read. I have now read through it. The implication was that there was a lot of transparency. At first, it seemed that that was the case, but, as you read more and more, you find that there are a lot of vague terms in the Bill that require a lot of head-scratching to try to understand exactly what may be meant. Trying to engage the public in understanding what the Bill says and what its

implications for them will be has been a challenge. There probably need to be many more readings of the Bill before you can get to the bottom of even a tip of what might have been meant.

Caroline Wilson Palow: I agree. We did and do welcome the opportunity to engage in this process. As we have started to get into the Bill, which is long and complex, we have started to notice a few things. For instance, Part 6 is about bulk powers, but when you look into some of the other particularly targeted provisions, you start to see that aspects of those look quite a lot like bulk powers in and of themselves. The service provider provisions that are sprinkled throughout the Bill put a lot of obligations on service providers, which I know you have often heard about, and which seem like they could undermine both security and trust. Those were not things that were necessarily apparent when we first took a look at the Bill. Another particular provision that concerns us a bit is Clause 188, on national security notices, and how that will play out in conjunction with the other provisions of the Bill.

Jim Killock: We have been particularly alarmed by the reintroduction of the so-called filter, which complements the collection of very widely defined Internet connection records. The filter seems to us to be essentially a federated database and search system, very much like previous incarnations of the Communications Data Bill, the snoopers' charter or the intercept modernisation programme. It has been proposed a number of times and stopped a number of times, because of the power to look into people's lives that it would give. In a sense, that deserves an entire debate on its own, as does the recent admission of collection and use of bulk datasets.

What is a bulk dataset? Which of them have been accessed and grabbed by GCHQ so far? To whom might that apply? Just about every business in the country operates a database with personal information in it. It could be Tesco Clubcard information. It could be Experian's data about people's financial transactions. It could be banking details. It could certainly be any government database that you care to mention. From that perspective, it is hard to see where surveillance ends as a result of bulk datasets. Traditionally, we have thought of surveillance as being about communications data and as being targeted. In this Bill, we have various measures for blanket collection—bulk collection, as it is referred to—and we extend that to any private or public institution that happens to have data. From that perspective, it is pretty worrying. It is hard to see the start and end of it.

One good thing that we did not necessarily expect is that there is a thorough or, at least, a large document spelling out the apparent operational case for Internet connection records. The fact that that has been produced is a welcome step. A very important thing to do when asking for a new power is to produce documentation explaining why it might be needed. That said, it again requires examination on its own behalf, as do the GCHQ powers. They need an operational case. Parliament has not debated why GCHQ has those powers; it has merely been presented as something that is happening and that we should now legitimise. In the USA, those kinds of powers were examined—bulk data collection and use under Section 215 of the Patriot Act. An operational case was made and was reviewed by bodies that were trusted by the President and by the USA's democratic institutions—the Privacy and Civil Liberties Oversight Board and the NSA review board. Both came back and said that there was no operational case for the bulk collection and use of data; nothing the NSA had done showed that that data had prevented anything significant. That kind of review needs

to happen here. The fact that it has happened in the USA and they have come up with the conclusion that these programmes need rolling back ought to be something that you consider carefully. Parliament really needs to examine those operational cases.

Q128 The Chairman: I think that I have got the message. I am assuming that you do not think that the Bill strikes the right balance between security and privacy. Without going into detail—my colleagues will ask questions on different parts of the legislation—other than dumping it altogether, do you think that it could be improved?

Shami Chakrabarti: It could certainly be improved. One thing we would all agree on, and would agree with the Government on, is that there needed to be a new Bill, in the light of Mr Snowden's breathtaking revelations. Whether you consider him a hero or a traitor, there is no doubt that he revealed practices and capabilities where we, the people of great democracies on both sides of the Atlantic and all over the world—I would include parliamentarians in that definition of the people—had little or no idea of the sheer scale of mass surveillance that was being conducted against populations. There is a debate to be had, of course, about how much of that should or should not happen, on what basis and with what safeguards, but in the light of that there had to be new legislation, because whatever was happening was happening, at best, on very creative interpretations of outmoded laws. Some of us would suggest that it was happening outside the law and without sufficient parliamentary scrutiny, public discourse and legal authority.

We certainly agree that there must be a new Bill; there must be something like this Bill. My fundamental objection is that too much of it is about sanctioning mass surveillance of entire populations and departing from traditional democratic norms of targeted, suspicion-based surveillance, for limited purposes. There are insufficient safeguards against abuse. For example, there is the argument that I know you have had extensively about the role of the judiciary. Our position is clear. This is not a system of judicial warrantry. This is Secretary of State warrantry, save in one of the most chilling provisions of the Bill, which is about hacking and the new concept in public understanding of what the authorities propose to do. We think that is one of the gravest powers, because potentially it leaves long-term damage to systems, individuals, devices and security, after a perhaps justifiable investigation. That has the lowest safeguard of all, because in certain circumstances it involves not even the Secretary of State but, for example, a chief constable. There is too much surveillance, there are too many people, it is not to a tight enough threshold or a high enough standard and there is insufficient authorisation by the independent judiciary.

Caroline Wilson Palow: Following on from that and your introduction to the question, security and privacy are not necessarily mutually exclusive. The hacking provision, in particular, shows that there is a lot of potential to undermine security by allowing that power, including the fact that the use of malware—the type of software that allows access to computers through hacking—is not necessarily well controlled. It is like breaking a lock on a door and leaving the lock broken, so that other people can potentially get in and access the same device or equipment that was targeted in the first place. That is an example, within equipment interference, of some of the security problems. There are also greater, overarching concerns about undermining things like encryption standards and whether or not that would be permissible, both under the hacking provision and under some of the provisions, like Clause 189, which say specifically that the removal of electronic protection could be required of service providers that are subject to compliance with warrants and

authorisations under the Bill. Finally, data retention in and of itself has certain security concerns. Of course, as we have recently seen with TalkTalk here or even the Office of Personnel Management in the US, there are breaches. When you are mandating companies or even Governments to keep more information, it makes the breach even worse when it happens.

Renate Samson: I support the points that have been made about concerns with regard to safeguards. Caroline made the point that privacy and security are two sides of the same coin. We also have to look at the idea of protection. Part of this Bill is about protecting the public, yet, as has been pointed out, there are other elements that will potentially make the public vulnerable, whether that is through equipment interference or through weakening of encryption, for example. We have to step back and have a think about what protections the public require with regard to the proposals in the Bill. The idea of full independent judicial authorisation is something that I know you have been discussing at length. I would support the view that it needs to be explored in a lot of detail. We are on the cusp of being complete digital citizens. We do not have a choice any longer about our engagement online. Proposals that suggest that online engagement can be surveilled at any time, potentially, and retained for a number of months are a worry to us all. It is not the case that the Bill should be scrapped, but there are certainly areas that need to be strengthened greatly.

Suella Fernandes: On the flipside of those comments, do you equally accept that the scale and nature of the threat that we currently face is unprecedented and severe?

Shami Chakrabarti: I do not doubt that the world faces enormous threats from crime, terrorism and so on. I do not think that any of us doubts that. The question is how best to counter those threats. I will repeat the previous remarks, which are really important. It is not about a trade-off between privacy and security. A lot of what we are concerned about is actually security. What is national security if not the personal and, increasingly, the personal cybersecurity in relation to where I am—whether somebody is in my house, engaging online, and whether I am away and, therefore, open to an attack or a burglary? My financial records and so on are part of my personal security and cybersecurity. National security is to some extent the combined personal and cybersecurity of millions of people. We think that up to 50 billion emails are intercepted every day by UK authorities. There are only 7 billion people in the world, and only 3 billion of them currently have access to this kind of technology. To me, that in itself is a threat to personal security—not because the authorities are malign, but because when you collect data and create vulnerabilities, that data can be attacked by non-governmental sources and the vulnerabilities that have been created can be attacked similarly.

Suella Fernandes: On the vulnerabilities you talk about, you point out the scale of, for example, communications data and equipment interference and interception, but those powers have been absolutely essential and critical to successful convictions for large-scale child sexual exploitation, human trafficking and serious and organised fraud and crime. Those are powers that are currently exercisable by our law enforcement services. The Bill represents a drawing together and consolidation of existing powers.

Jim Killock: We are talking about several different things here. There are policing powers, there are data retention powers and there is extension of those for the police in the ICRs and the filter, so you have that body. Then you have the other area around GCHQ—what it does and how it gathers information. You have to look at both of those quite separately.

You are really asking about the operational case. As I said, my problem with the operational case is that it has not been presented to anybody for GCHQ. When the equivalent was done in the USA, the President of the USA and its democratic institutions decided that there was not really a case for a lot of it and decided to roll it back, because it was essentially purposeless. Here we have an operational case for the police with regard to ICRs, but we do not have the mechanisms, because we do not have a civil liberties board in the UK. It has not been constituted, despite potentially being put into law. That has not been examined.

On data retention in general, we have had a ratcheting back of data retention in a lot of Europe. These apparently essential tools have not been operational for a long time in Germany, the Czech Republic, Slovakia and a number of other places. There are about six or seven countries where these sorts of programmes have essentially been cancelled. There has not been a concomitant outcry from the police that they are no longer able to solve crimes and that there is spiralling dysfunction in the police. That has not occurred. Something to bear in mind is that there are often several routes to solving crimes. Data, through data retention or collection, is only one. That data probably resides on laptops and mobile phones. It will reside at service providers. That is talking only about the data side of it; there will be other kinds of factors in the equation. It would be interesting to hear from Caroline about data preservation and the standards elsewhere.

Caroline Wilson Palow: The US, for instance, does not have a data retention provision, yet it is still able to solve crimes. In fact, it uses mechanisms like data preservation orders, which are much more targeted, are not across the board and can be quite effective. You also have instances, which have been mentioned, of places like Germany, the Czech Republic and other countries in Europe where data retention is either much more circumscribed or non-existent. Again, we have not seen a collapse due to the fact that it is not there.

To pick up another point you asked about—the existing powers, particularly in the context of equipment interference—it is true that it was revealed earlier this year that the intelligence services were engaging in hacking and, when this Bill was introduced, that law enforcement, too, was engaged in hacking. Until that point, that had not been revealed publicly. The reliance on the Intelligence Services Act and the Police Act, which are incredibly broad powers, to say that that was already in statute is inappropriate, because they are so broad. There was no indication that it was actually happening. Since those Acts are from 1994 and 1997, if there was an indication in the Acts that hacking was possible, why was there concern not to reveal it sooner? Why was the position of the Government until earlier this year neither to confirm nor to deny that those powers were being used? While they may have been in use, they have not actually been in law up to this point. That is why we talk about them as new powers in this Bill.

Shami Chakrabarti: I have one further small point on comparative practice around the world and the importance of law enforcement. There is still no provision for intercept

evidence to be admissible in criminal proceedings. There has been and is to be all this interception, for laudable criminal justice purposes—public protection and law enforcement—but there is still not the provision, for which some of us have asked for many years, for interception, when it is proportionately and lawfully gained, to be used in criminal prosecutions, as is the case all over the democratic world and among our allies.

The Chairman: Thank you. I move to Dr Murrison.

Q129 Dr Andrew Murrison: I am getting the sense that you are not convinced that the "double-lock" provision, about which much has been spoken in recent weeks and on which much store has been put by those who have been involved in bringing the Bill to the position it is currently at, is really much cop. However, I believe that it is likely to remain a feature. Given that it is likely, what do you think could be done to improve the double lock? Would you see virtue, for example, in distinguishing national security from serious crime, having the double lock apply to national security and having judicial authorisation only for serious crime? Would you see virtue in, for example, a different means of appointing the information commissioners who will be involved in this process?

Shami Chakrabarti: Some of my colleagues are the great technologists and experts. I am just a humble lawyer in recovery—or in remission—so I find it easier to make the analogy with the real world when I am dealing with the virtual one. We are digital citizens, but we are still people and citizens. If I want to search your house or your office for laudable reasons, I go to a magistrate for a warrant. I can understand the argument coming from the Government that when we are doing this national security stuff and, perhaps, spying on foreign Governments, we cannot just go to any old magistrate. There has to be a double lock, surely, on something as serious as interfering with the German Chancellor's communications. That is such a political decision that there ought to be some Executive involvement. The double lock is simple: have a provision across the board for judicial warrantry, but as an internal administrative matter, make sure that those warrants are not sought by the authorities unless they have been to the Home Secretary first. In the non-crime cases—the international relations/national security cases—as a matter of good public administration, go to a Secretary of State first, but always have the sign-off to protect people's rights and freedoms, whether in the UK or around the world. Have that sign-off by a judge, as you would for your home, your flat or your office. Again, that is the practice across the democratic world.

Renate Samson: I second that. A large part of what we find ourselves doing when it comes to the digital world is incomprehensible to most of us, because it is invisible, yet we all understand what happens when somebody knocks at our door and asks to have a look around because they suspect us of something, and that element of being suspected of something is important. The real world understands a judge signing off on something. The general public have confidence that there is independence to it. While we may currently have a benign Government, we do not know what the future holds. This piece of legislation should hold up for many years. We do not know what the future will bring, so independence is hugely important. That will also mean how the judges are appointed. To feel genuinely that surveillance conducted upon us is being assessed independently and with no interference from anywhere else will reassure the general public that, should the

rest of the provisions in the Bill become law, they will be secure and thoroughly thought through, not just signed off with a flick of a Minister's pen.

The Chairman: It is said that a Secretary of State is ultimately accountable to Parliament for his or her actions, whereas a judge is not. What is your view on that?

Renate Samson: You took evidence at the beginning of this week from Mr Paterson and Lord Blunkett. I think that they answered that question for you, in that neither of them has ever stood up in Parliament and talked about a warrant they have been involved in signing off.

Jim Killock: It is also worth reminding ourselves how we got here, in a sense. The Regulation of Investigatory Powers Act had powers for the collection of material from persons overseas. The meaning of that warrantry system was extended through practice to mean every communication passing between the UK and the USA. That is how the Tempora system of bulk collection was created—through those warrants, which were politically authorised. There was a political decision, alone, to extend the meaning of those RIPA warrants, which meant that essentially Parliament was cut out of the decision, right or wrong, to engage in the programmes of bulk collection of data that we are now authorising in this Bill. It seems to me that if one is to restrain the Executive from creative interpretations of the statutes, as Shami said, you need that judicial authorisation. They should be saying, "Minister, I do not think that this is necessarily how the system was designed to work. Perhaps you might like to consult Parliament". That is a far more likely outcome than the Home Secretary saying to GCHQ, "No, I am going to deny you those powers for one or two years while I work out a political opportunity to legislate".

Caroline Wilson Palow: In conjunction with that point, it means that the judicial commissioners need the full ability to assess the warrants when they come to them. It should not be just a judicial review standard. They need to assess fully the substance of the warrant and, among other things, whether there are other less obtrusive means by which this information could be obtained. That is an easy edit to the Bill. Every time the judicial review provisions appear—it is at subsection (2) of most of those clauses—you just delete it. You take it out.

Suella Fernandes: Are you saying that the double lock and the judicial involvement strike the right balance in having judicial review as an element of the decision-making process, or are you saying that it should not be there?

Shami Chakrabarti: Judicial review does not help at all in this context. When you are deciding whether it is proportionate to issue a warrant for intrusive surveillance of an individual, let alone of a whole group of people, that is a judgment made on the evidence. A judicial review test only second-guesses the Secretary of State, in very limited circumstances. Did they make a bonkers decision that no reasonable Secretary of State could take? That is not judicial warrantry. In the statute there should be a one-stage test: the judge signs the warrant. However, because people are concerned about cases of interception on foreign powers, for example, which is classically a matter for the Executive rather than for independent judges, police officers or whatever, interception and so on of foreign statesmen and powers should go to the Home Secretary first, as a matter of good

public administration. You would not even need that in the statute, or you could put it in the statute for that category of case.

Renate Samson: Your question is interesting. I have listened to a number of the sessions of evidence that you have taken. You have all posed the question a number of times, "What exactly is meant by judicial review?". Witnesses have given you a variety of versions of what judicial review means. There is lack of clarity.

Suella Fernandes: That is exactly what I was going to raise in my question. You will agree that, with judicial review, the judge would have access to the same information as the Secretary of State or the Minister.

Shami Chakrabarti: I do not think that is suggested in the Bill. There is nothing to suggest that.

Suella Fernandes: That is what judicial review involves, does it not?

Shami Chakrabarti: No, it does not. This is a term of art. A judicial review test, as a matter of our law, is a very limited opportunity for a judge to second-guess a decision that has been made by a public authority, whether it is a Secretary of State, local government or whatever. It is not a double lock.

Jim Killock: Basically, it is, "How did you follow procedure?", is it not?

Shami Chakrabarti: Yes. Did you make a decision that was within the realms of a reasonable decision? Could any reasonable Secretary of State possibly have made that decision? It is not appropriate for warrantry.

Suella Fernandes: What about the proportionality test, which involves balancing the right infringed and the objective met? That goes further than what you are suggesting, does it not?

Shami Chakrabarti: But that has not been allowed to the judge, under the provisions of the Bill. They are not second-guessing the Home Secretary's decision on the merits of proportionality, under the Bill.

Caroline Wilson Palow: That is exactly our concern. When you talk about judicial review, all you are doing is looking to see whether proportionality has been assessed by the Secretary of State. The judge will not have the power to say, "You have made that assessment incorrectly". In the US, to give an example of a comparison between two different types of warrantry there, a normal warrant would go directly to the judge. There is a political consideration that is made ahead of time. For instance, the US attorneys, who are the federal attorneys who often start the process, are politically appointed and will make a decision about whether or not to seek a warrant in the first place. Once that is done, it goes directly to the judge.

Suella Fernandes: Before we finish this line of questioning—I know that other people want to get in—I need to put on the record that the statute states explicitly that it must be "proportionate" and "necessary". That is the relevant test.

Shami Chakrabarti: You have to look at Clause 19(2).

Caroline Wilson Palow: The concern is the way in which the two play together. That is why I said that we think you should just delete subsection (2). We totally agree that necessity and proportionality need to be assessed, but, once subsection (2) is in there, it reduces the ability of the judicial commissioners to make that assessment. To continue the parallel that I was trying to draw, in the US there has been a lot of talk about the FIS Court, which acts on foreign intelligence. This is PRISM—the types of authorisations for collecting intelligence on people around the world. Its powers are the equivalent of what judicial review would be here. Essentially, when a request comes to it, it has to check the box to say that everything has been considered as necessary, but it does not necessarily get to question the conclusions that were reached by the person who was seeking the warrant in the first place.

Shami Chakrabarti: A double lock would mean, "I can substitute my decision on the merits for yours". Traditional judicial review means, "I look at the way you made your decision, but I do not substitute my own for yours". You have to be procedurally irregular or to have made a completely insane decision that no Secretary of State could make. That is achieved by Clause 19(2), otherwise there would be no purpose to it.

Matt Warman: We have had an awful lot of witnesses tell us that their expectation and understanding of what the Bill says regarding judicial review would, as Suella Fernandes has said, in fact mean a test that looked at the evidence. It would have to be proportionate and go through all those things. You are saying simply that that is not your understanding of judicial review. It therefore seems to me that we are talking simply about definitions; we are not actually talking about a principle, because what we have been told is what you are saying you are asking for.

Shami Chakrabarti: It just does not stand up in law. These are well-tested terms. If you want to create a full merits appeal in statute, there are many precedents for doing that. You do not put in a clause like 19(2); you can do it much more simply. I believe that you will hear from the Secretary of State in the not-too-distant future. You can just ask her: "Is it your view that you will make an initial decision and there will be a full merits review? The judge can just second-guess your decision and make a different one. Is that your intention?". If she says that that is her intention, that will help for Pepper v Hart purposes, but there are far clearer ways to deal with it, like just deleting Clause 19(2).

The Chairman: Thank you. Can I move to Mr McDonald?

Q130 Stuart C McDonald: I have another million-dollar question. What is your understanding of the meaning of the term "Internet connection record"? Why would their gathering and analysis be more intrusive than for other forms of communications data?

Shami Chakrabarti: This has been quite a journey for me. I have had lots of younger and more technologically savvy colleagues explain the sheer scale of what we might be looking at as regards Internet connection records. If you take your favourite device—your smartphone, your tablet or just the sites you go to from your laptop or desktop—we are looking at things like the websites you visit. We are looking at the communications software that you might use to speak to your mother—Skype, WhatsApp and so on. We are looking at all the icons on your menu, such as your Twitter and your diary. Recently a health one popped up on my phone uninvited, telling me how many steps I took yesterday. Taxis,

maps; the list goes on. Photos, my Internet shopping, banking apps—I understand that all those things are potentially within the broad concept of Internet connection records. As we look just a little way into the future, in the discussion that people describe of the Internet of things, more and more of our real lives will be managed online. Now we will be talking more and more about the little icons on our devices that connect to our fridges, our cars, our burglar alarms, our gaming devices and so on, so the separation between my real-world security and privacy and my cybersecurity and privacy is almost completely collapsed. This is very intrusive on millions and millions of, for the most part, completely innocent people.

Renate Samson: It comes back to the point that I made that we are all now digital citizens. It is that—it is life. It may feel at the moment that it is just a mobile phone and a laptop, but, as Shami explained, with the Internet of things it will be everything. That will create a huge amount of data that will be constantly ticking over. We have been informed that the Internet connection records are just the URL, before the first slash, of a website and no content, but from the technical evidence I have been listening to and you have been receiving, and from all the different things that I have read, which Jim will probably be able to explain better, I am not entirely sure that it is quite as clear-cut as has been implied. I would certainly like to hear from the Home Office—from government—with regard to this Bill a very clear definition that it knows exactly how this can be done, because I am not sure that I do.

Jim Killock: It seems to me that essentially the Internet connection record starts from the point of view that the Home Office wants the power to have retained the fact of somebody using the Internet, with some other service, and to record that. It has decided that the best way to do that, given how much the Internet is used, the purposes it might be put to in the future and the services that might appear, is just to say, "Let's have a very broad definition of anything that connects to anything, whether it is a person or a machine. That will allow us to compel Internet service providers to collect information about anything we deem important in the future".

I do not think that is really a good way to legislate. It is incredibly broad, it is open to abuse and the cost implications are impossible to put a number on. If you have power to collect and retain any information, no matter how difficult that is and how much of it there is, essentially you have just written a blank cheque to scale up surveillance indefinitely. Of course, once you have an initial investment and the thing has started to roll out, that poses the problem of how you restrain it in the future when it turns out to be not quite as useful as you hoped. Do you pour in another few tens of millions of pounds to extend the amount of information that you are collecting under this very broad power? Given that the companies will probably tell the Government that it will be more effective if they spend that extra bit of money, this seems to be a financially haphazard way of working, as well as haphazard in terms of human rights and the proportionality of the surveillance we are authorising.

Caroline Wilson Palow: This is quite a confusing definition, because essentially you have two different definitions in the Bill. You have Part 3, where Internet connection records are explicitly mentioned, but in Part 4, under data retention, you have a clause that, under the commentary, is supposed also to encompass Internet connection records. The definitions

do not completely align, and for that reason we are somewhat confused about what Internet connection records really are.

Let us take an example from the commentary that Renate has already mentioned—the idea of taking the domain name of a website, which is the information before the first slash. Potentially, that could be quite intrusive and could reveal a whole lot of information. It is not as innocuous as just bbc.co.uk, which is the example that they gave. For instance, that domain name could be saveyourmarriagelikeme.net or domesticviolenceservices.com. Maybe one of the most interesting ones is crimestoppers-uk.org. This is where you can make anonymous tips to help to solve crimes. Of course, if you had the Internet connection record that said that someone had gone to crimestoppers-uk.org and you also knew the time when the tip had come in—if you were the police, for instance—you could very easily figure out who had put in that tip. That is a real problem, because if you are destroying that anonymity you can undermine the ability to solve crime.

Q131 Mr David Hanson: This is the central question many of us will have to wrestle with. Surely the police, the security services or whoever accesses that, under authority, with judicial review, is doing so only because there is some potential link to a potential investigation. The vast majority of people will never have that link checked or looked at. I am wrestling with that myself. I want to get your assessment of whether the proportionality is there. If we do not collect the information, none of those leads can be followed up.

Shami Chakrabarti: You are collecting huge amounts of sensitive information that is not currently collected and, therefore, you are creating the vulnerability I am so concerned about. I am not even talking at the moment about potential abuses by the authorities. I am talking about the vulnerability to hacking by other people that you create when you create a massive sensitive database and put the entire population's online life under surveillance in this way.

Renate Samson: My understanding is that this would help to support requests that are already made for communications data. At the end of November, IOCCO published as a starting point to a further publication a breakdown of 100,000 communications data requests by 29 police authorities, including the National Crime Agency; 46% of those requests related to burglary, robbery, theft and drug offences. If this is to support that, people may see it very much as an intrusion. On that sort of issue of crime, why do you need to know what website somebody has looked at with regard to burglary? We have to think about the intrusion into people's lives, based on us as digital citizens, before we start to discuss the retention and use of Internet connection records. Their retention is an issue I know you have looked at, but off the back of the TalkTalk hack, for example, we need a lot more clarity on how companies will be asked to store that data to ensure that they are safe.

Jim Killock: You also have to consider the wider effects on society. If I said to you, "When you go home, can you note when you got home and which newspaper you read, although do not worry which article it was? If you ring your family this evening, make a note of that and then tomorrow, hand it into the police", you would think that an excessive ask.

Shami Chakrabarti: And every hotelier, every restaurant owner, every pub, every cinema and every theatre that you enter will be required to keep a record of when and where you entered. That is the equivalent of what is being proposed.

Jim Killock: The question then is, is that a proportionate thing? What are we trying to solve? Is it quite as desperate a situation as is being claimed? As I said, these powers do not exist in other democratic countries. Russia has just been given a bit of a rap for similar sorts of activity. A number of European countries have rolled back on traditional data retention, never mind this kind of extension.

The Chairman: Lord Strasburger?

Lord Strasburger: My point has just been covered.

Q132 Stuart C McDonald: Are there other ways to go about IP resolution that are less troubling? The Home Office and law enforcement agencies will say that retention of these connection records is essential for that to be successful.

Jim Killock: One thing that you have to ask is whether the technology will out-evolve this. Will IPv6 catch up with some of the problems that it is currently seeing? You also have to ask how the Internet might work in the future and whether any of this will work. Some of the evidence that has been put about is quite interesting. People have said, "How do we know whether somebody has used Twitter or Facebook? We need to know in emergencies whether somebody has been accessing that website". Phones just do that now every couple of minutes. If they are constantly connecting to all these services, you will just have a huge glut of information that is not a fat lot of use to anybody.

Q133 Matt Warman: One of my frustrations with this conversation is that it is always said that the Government are being asked to hold this stuff. Actually, we are asking ISPs to hold it. That is a very important distinction that we need to continue to make. Law enforcement agencies tell us that they want access to the information and are happy for it to be held externally. You seem to be saying that you are not happy with that. I wonder what alternative you would propose.

Jim Killock: It may not be a government-held database, but it is a series of data centres that are all accessible by a single mechanism that can then be queried in parallel from an officer's desk.

Matt Warman: With appropriate oversight.

Jim Killock: There are some interesting things there. It seems that the way it will work is that you can get an officer to ask the computer whether it has any useful information in a case. It will tell you the things that it might have, and then you can go off and get some warrantry for it. It is almost saying, "We will go not on fishing expeditions, but if you did, here are the results you would get. Why don't you have a think about whether or not that is useful?".

Renate Samson: You say that there will be appropriate oversight. Currently the Bill will retain the process that we have now. From Big Brother Watch's point of view, that is not

appropriate oversight. We would like to see a further layer of independent judicial approval and authorisation of an internally signed-off warrant.

Matt Warman: The point I was making is that it is not a free bucket any policeman can look at.

Renate Samson: We also have to acknowledge the recent case with regard to Police Scotland and on which IOCCO reported, where warrants were being signed off and misused.

Matt Warman: Misused being the operative point.

Renate Samson: Yes.

Shami Chakrabarti: Sometimes that will happen. To go back to the real-world analogy, when I said that this is the online equivalent of requiring all those businesses—hoteliers, restaurants, cinemas and so on—to keep a detailed record that they do not currently keep of everybody's comings and goings, that does not mean that I am against ever putting a particular hotel, restaurant, gym or whatever under surveillance. I just think that you take a targeted approach. When you get suspicion that conspiracies are being conducted in a particular room above a particular pub, at that point you put that site under surveillance. Then you put the people who have been to that site under surveillance. That is the kind of approach we should continue with in our democracy, in the virtual world as well as the real one. If you have concerns about particular activity and sites, you can go to ISPs and CSPs and ask for the data they currently hold anyway. You can seize people's devices, because those people or organisations have now come under suspicion. You can target suspicion not just around individual people but around organisations and, indeed, websites.

Renate Samson: I want to clarify your point about misuse. IOCCO is very clear that judicial approval was not obtained to acquire the communications data. My point, and the point of Big Brother Watch, is that independent oversight and authorisation of an internally signed-off warrant for communications data would, I hope, potentially ensure that misuse did not occur. That is just for clarity.

Jim Killock: The important thing is why we have the idea that necessary and proportionate surveillance is essentially targeted, rather than blanket. Why do we have that rule? Why has that been pushed forward? It is easy to imagine that in the UK we will never have any problems with our democratic institutions, the police will never overstep the mark and we can solve all this through authorisation regimes. However, if you look over the sea in France, you have the potential of a Front National Government, with parallel powers. You have powers similar to these in China and Russia. Is it the role of the UK to say that blanket surveillance, easy profiling and access to everything that everyone does in their lives is the right international standard to set and is absolutely, 100%, guaranteed never to turn into a problem in this country, or should we restrain surveillance to somewhere we can trust, for ourselves, for other people and for the long term?

The Chairman: Can I move to Lord Butler?

Q134 Lord Butler of Brockwell: I want to ask you about equipment interference. You have made reference to that. As I understand it, you are not claiming that equipment interference in the past has been non-statutory. You are claiming that, although there are statutory powers, they are very general, they have been widely interpreted and the public have not been aware of what is going on. Do I have your argument right?

Shami Chakrabarti: You do have my argument right. I do not believe that equipment interference was necessarily in the mind of the legislators when the provisions that are now being relied on were passed. Those provisions were more about traditional breaking and entering, bugging and so on. I certainly do not think that the public understood in that way the activity that was being justified ex post facto. That creates a problem for Article 8 of the convention, which requires a certain level of public understanding for something to be law for the purposes of the ECHR. Those powers were there and they were used for more traditional interferences, but hacking is a very, very serious business. It is more than just surveillance, because you are potentially changing data and causing long-term damage to data security. I am not saying that it should never be allowed, because that would be like saying that you should never break and enter in order to find the hostage, the terrorists and so on; I just think that there should be much tighter safeguards for hacking in the Bill. Again, in principle, it should be a targeted approach, not a blanket one.

Jim Killock: It is worth remembering that the hacking power has already caused some very significant problems. You probably remember that Belgacom, the telecoms provider in Belgium, was hacked by GCHQ, allegedly. In the first month of the clean-up, that cost it around £15 million. A series of telecoms providers, including Deutsche Telekom, were also hacked by GCHQ. Those are law-abiding companies. They are not terrorists. They have information and are a conduit to further information, perhaps, but they are also people who can be compelled to co-operate with their own national authorities. However, GCHQ, under this warrantry and hacking regime, has instead taken the view that foreign, legitimate companies with international stature, within the bounds of Europe where we have common laws and systems, are a legitimate target for hacking, and that the clean-up operations are, frankly, not our concern.

Lord Butler of Brockwell: Could we stay within the UK for the moment?

Jim Killock: But this is a UK operation.

Lord Butler of Brockwell: I know that it is a UK operation. I am just talking about the targets at the moment. The point that you have made is about overseas targets. That is a separate consideration. Within the UK, you must agree that it is an advance that this proposed Bill gives specific authority for and introduces transparency into that power.

Shami Chakrabarti: I agree with that. I wou*l*d just like it to be more tightly regulated, given the consequences.

Lord Butler of Brockwell: Sure. You are not arguing, are you, that such a power, properly warranted—we have had discussions about what proper warranting is—may not be a legitimate weapon?

Shami Chakrabarti: In extremis. The intrusion is graver, because it is not just surveillance but actual damage—not least, potentially, damage to fair trials, if now every criminal defence lawyer can argue, "This isn't a genuine email. This isn't genuine data any more, because of hacking capacities". Given how serious the consequences of hacking are, the thresholds possibly need to be even higher than for other powers in the Bill.

The Chairman: I will now move to Lady Browning and Lord Henley. I am conscious that there is a vote in the Commons at 7 pm, but I would very much like the Commons members to be here for the questioning.

Q135 Baroness Browning: You have all expressed concern about Clause 189. I wonder whether you could share with us what you believe the effects will be on both service providers and customers. Ms Wilson Palow, your submission stated very clearly your concern about this.

Caroline Wilson Palow: It is a very broad power, to begin with. Essentially, it says that obligations can be placed on service providers to facilitate interception, hacking or any other power in the Bill, and they would need to take those steps ahead of time, before an authorisation or warrant was placed. Within that broad power, there are some examples of what might be done. A particular concern of ours is the removal of electronic protection. We interpret that as the potential to undermine encryption. Encryption is crucial to so much of what we do all the time, including all our financial transactions. It gives us the security to operate online. The removal of encryption has the potential to undermine all of that. We think that the balance there has not been struck appropriately.

Shami Chakrabarti: Taking my real-world analogy again, because of my poor understanding of these things, I do not think that it would be proportionate to give government the authority to demand that every locksmith in the country makes a spare key every time he is setting a lock for a home, a property or whatever. It is proportionate in certain circumstances, under warrantry, for the authorities—the police—to break into a targeted property because we believe that there are explosives, contraband or evidence there. To ban privacy, to ban private conversations and to require people who live on trust—companies that are all about creating a space of trust, so that we can have trust in our banking system et cetera—to leave those gaps in the nation's cybersecurity is quite problematic.

Renate Samson: It is the point that we were making earlier. The Bill is about protecting society. Encryption enables the protection of society. It enables people to use Crimestoppers. It enables whistleblowers to lay clear things that are going on that benefit society. It enables the vulnerable to communicate safely. Battered wives, for want of a worse expression, can ensure that they communicate as necessary. People on witness protection programmes can have an element of safety. It is much broader. It involves all of business. When all the communications in our home and everything else we have talked about on the Internet of things are connected online, we all want to know that our energy can be supplied safely. Encryption, as our submission to you explains, is not just a concern of privacy campaigners. It is a concern of Governments and business and one that will impact on us all, as all our lives are lived online.

The Chairman: Thank you very much. I move now to Lord Henley, on the Wilson doctrine and other matters.

Q136 Lord Henley: There is protection in the draft Bill for legally protected communications of journalists and journalists' sources, and there are protections for Members of Parliament of both Houses, enshrining the Wilson doctrine. Do you think that the Bill goes far enough?

Shami Chakrabarti: Not at all. There is room for some serious improvement. Let me be positive: there is room for real improvement. As far as I can tell, the Wilson doctrine has been completely reneged on. Recent statements by the Prime Minister suggest that, effectively, there is no Wilson doctrine in practice any more.

Lord Henley: What particular comments of the Prime Minister are you referring to?

Shami Chakrabarti: My understanding of recent statements from the Prime Minister is that there is now no absolute practice of not intercepting parliamentarians' communications. That was an absolute promise that came from Prime Minister Wilson and, indeed, was repeated by subsequent Prime Ministers.

Lord Butler of Brockwell: No. I am sorry, but you are wrong about that.

Shami Chakrabarti: I have read the Wilson statement. As regards what could be improved, I accept that there could be certain very rare circumstances where it would be justifiable, in a democracy, to interfere with even the communications of parliamentarians, lawyers and journalists, but we want something closer to the provisions that you currently have in place for production orders. You want something approaching reasonable grounds for believing that a very serious criminal offence is happening or has happened, and that there are no alternative ways of getting to the evidence; otherwise there are real dangers. Think of the political dangers. Perhaps it was just a rhetorical flourish, but we have had leaders of parties suggest that opposition parties are a threat to national security. I do not think that it is healthy for democracy for opposition political parties to believe that it is possible that they can be intercepted just on the say-so of a political opponent, even if that political opponent is the Prime Minister.

When it comes to legal professional privilege, we now know, because of the Belhaj case, that the security agencies were looking at legally privileged material that was relevant to a case being brought against them in relation to torture. There need to be much graver safeguards—we are back to judicial warrantry—and a very strong presumption against looking at parliamentarians' communications, legally privileged communications and journalists' sources.

The Chairman: Thank you very much. I will give you just one or two more minutes, because I want to wrap up with a couple of suggestions about how you can give us more evidence.

Jim Killock: I want to say something very specific about this. It is very hard to tell where the boundary between journalist and non-journalist lies. In this day and age, it is not somebody who is working on a paper; it could be somebody writing a blog and self-publishing. Many NGOs have a similar role to journalists in exposing, commenting and publishing. Particularly with communications data, where the system sometimes has to go to a magistrate or

whatever and sometimes has to be self-authorised within the police, it breaks down when you have this blurring, which is a very strong reason why all authorisation should be done by an independent authority. That, in particular, has been spelt out in the data retention judgment by the CJEU; when communications data are accessed—in that case, it was talking about retained data—there should be independent authorisation. This is one of the reasons why.

The Chairman: Thank you very much. It has been a fascinating session. It really has—very revealing. If in the evidence that you present to us you want to go into some of the detail of any amendments or drafting issues that you feel would improve the Bill, which you mentioned earlier, please feel free to do so and send those suggestions to us. Thank you very much for coming along today.

Clare Ringshaw-Dowle, Chief Surveillance Inspector (QQ 47-60)

Evidence heard in public Questions 47-60

Oral Evidence

Taken before the Joint Committee

on Wednesday 2 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Stuart C McDonald MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Bishop of Chester, Lord Hart of Chilton, Lord Henley, Lord Strasburger.

Witness: **Clare Ringshaw-Dowle**, Chief Surveillance Inspector, gave evidence.

Q47 **The Chairman:** Lord Judge, Sir Stanley and your staff, thank you very much indeed for coming along to us this afternoon. As you know, this is a very important Bill. The Prime Minister described it as the most important of this Session. Much of the Bill refers to the change in oversight provision, so we are very grateful for your coming along. I wonder whether you want to say anything yourselves before we start asking some questions.

Lord Judge: I would like to say something, particularly in view of the discussion that has been going on with Sir Mark. I cannot think that anyone would have designed the present three-bodied system. It would never have happened; it should not have done. We work piecemeal on the legislation; we produce piecemeal results; and we have produced three bodies, all of which have responsibilities in the broad sense that we are talking about and all of which work in different ways.

Let me give you some "for instances". Sir Mark has just given evidence to you. He is the commissioner. He has no inspectors. Sir Stanley will tell you that he is the commissioner and, with his team, he has 10 inspectors. I will tell you that I have taken over the surveillance commission. I have seven inspectors, who are former police officers of no less than superintendent level, a Chief Surveillance Inspector, six commissioners, three assistant surveillance commissioners and, good heavens, there is even me. We all operate differently. The focus so far has been on Sir Mark, and I know that IOCCO, as it is called, has had quite a lot of input, but can I just explain to you how this leads to confusion and can be improved?

The Chairman: Please do.

Lord Judge: We have had to take on oversight and prior approval of undercover police authorisations. We all know about the relatively recent disasters caused by officers going wrong in undercover operations. There is an application to us and, mark this: we have to authorise. Neither of the other two Commissions authorises. Every single piece of intrusive surveillance, certain types of property interference and long term undercover operatives

for which we are responsible is authorised in advance by a commissioner, who is a former judge.

The case is made out to us that there should be an undercover police officer in this particular, rather serious drugs case. The authorisation is made. In goes this brave young man or woman—and most of them are very brave young men and women—and they discover that there is quite a lot going on and it would be a good idea to have some intrusive surveillance, say into a car that is being used to transport the proceeds of drugs. He has to go back to his authorising officer. The authorising officer comes to us, and there is another application for intrusive surveillance to take place. That takes place, and that reveals something else: these drugs are actually to do with a potential terrorist ring.

That does not come to us; that goes to Sir Mark, but there is no pre-authorisation by him. Somebody says, "We had better have some communications input". That goes to Sir Stanley. There is no pre-authorisation by him. Now, I am sorry to say this, but telling the story the way I have is entirely accurate. If you thought about it, you would say, "Is this really the way we are doing business?".

Speaking only for my own team, every authorisation is made before any of the aforementioned intrusion takes place. The papers come to us, and I have a complaint about the quality of our equipment, but that is another question. A judge commissioner looks at them. He decides whether necessity is established and whether it is proportionate, which involves looking at the nature of the offence. You would not authorise intrusive surveillance for somebody who was stealing a tin of salmon from a supermarket. You are looking at sentences starting in the three to four-year range and upwards. He checks for proportionality: is this a reasonable way to go about sorting this problem out? He authorises or does not, or says, "I want more information". Then the process goes through.

At the other end of the process, every year my inspectors go in and conduct an inspection of every single police force in the country, Her Majesty's Revenue & Customs and so on—all the law enforcement bodies. They conduct random analyses inspections of all the things for which the body is responsible, such as encryption. There are all sorts of different things that come under the remit of covert surveillance. They then write a report. The report is written to me. It goes to the chief constable. I write my own report to the chief constable. Sometimes I say, "This is being very well handled. Your authorising officers are well trained. The paperwork is very good. The explanations are excellent", and so on and so forth. I have just written a very rude letter saying, "This is not good enough. You are not complying. There are too many breaches. There is too much inefficiency in this part or that part", or whatever it is.

I write that to the Chief Constable, and then I go and see him, or one of my commissioners does. I go to all the big Forces. We discuss the report for the year. Most of the time—and this I hope does not surprise you—the chief constables are as anxious as we are that the job should be done properly. Apart from the reputational matter, they are men, and women now, who want the job done lawfully. They are also aware of the dangers of evidence being excluded at the trial process or an abuse of process argument leading to the whole prosecution being discontinued. I go there; we discuss it. If I am unhappy, I will go again. I have not had to, but I have only been in this job for a relatively short time.

I am not recommending it to you, but our system is very different from the one you have been discussing with Sir Mark, and from Sir Stanley's. The idea that we should have a surveillance system in which there are three different bodies is itself absurd, and then three different bodies operating differently strikes me as daft. That is my opening statement.

The Chairman: Very interesting it was, too. Sir Stanley, do you want to make any comments?

Sir Stanley Burnton: As you know, I am the new boy on the block. I have the good fortune to have staff who have received a glowing report from David Anderson, as you will have seen. They have a range of competencies, including computer abilities. There were questions asked of Sir Mark about training. I have some computer knowledge; I was judge in charge of IT, but I could not go into a public authority and interrogate their computer system. We have inspectors who can and do just that.

We carry out an audit function. I believe that you cannot carry out an audit function properly unless you have some understanding of the business you are auditing. That does not mean to say you could do it yourself. I could not go into a computer and interrogate it to see how many search or interception warrants had been issued, and view the grounds and so on. But I like to think I have a sufficient understanding of what staff can do, and do, to carry out the functions of my office.

Like Sir Mark, as far as I am aware, there was no special security clearance carried out when I was appointed. On the other hand, when I was a judge, I used to do Special Immigration Appeals Commission, or SIAC, cases, which concerned terrorism and people who were alleged to be terrorists, so I have some acquaintance with that part of the job. Of course, I did criminal work, so I have some acquaintance with that area as well.

Q48 **Lord Butler of Brockwell:** May we take it from Lord Judge's and Sir Stanley's opening statements that you think it is a good idea that this Bill in future sets up a single Investigatory Powers Commissioner?

Lord Judge: I have no doubt about that. We also have to make all the three current bits of the system work in the same way. I personally think, although I have no experience of IOCCO or Sir Mark's work, that the authorisation process is one of the strengths of what we do. You have to have an authorising officer who persuades you that this is appropriate—i.e. necessary and proportionate.

Lord Butler of Brockwell: If I may then clarify my understanding of this, in your area, Lord Judge, there is pre-event judicial authorisation.

Lord Judge: Of every item of intrusion that comes within our jurisdiction for prior approval by a Surveillance Commissioner.

Lord Butler of Brockwell: In Sir Stanley's area, this Bill will set up, except in the most urgent cases, pre-event judicial authorisation. Is that correct?

Jo Cavan: It will in relation to interception warrants, but it will not in relation to acquisition and disclosure of communications data, which is the bulk of our remit. Around 500,000 requests for communications data are made on an annual basis, by a rather large number

of public authorities. The judicial authorisation and the double lock that the Bill introduces are only in relation to the interception warrants, of which there are around 2,700 a year.

Lord Butler of Brockwell: Thank you very much. Then, if I understood what Sir Mark said, in the case, however, of somebody placing a bug in premises, there will be no judicial pre-event authorisation. There will be a warrant, but there will not be a judicial pre-event authorisation.

Lord Judge: If it is an application under part 3 of The Police Act 1997, which we deal with a lot, there will have been a pre-judicial authorisation in advance (for activity in a private vehicle or premises). This is why the system desperately needs to be shaken up.

Lord Butler of Brockwell: What about in the case of the intelligence agencies? Did I misunderstand Sir Mark?

Lord Judge: No, you did not. The intelligence agencies work differently. If it is an ordinary police investigation, yes, every piece of intrusive surveillance is pre-authorised. In the case of intelligence, it works differently.

Lord Butler of Brockwell: In the case of an intelligence agency, at the moment and under the Bill as proposed, there is no pre-event judicial authorisation of the warrant.

Lord Judge: No.

Q49 **Suella Fernandes:** What do you think about the safeguards provided in the new system as compared to the current one? Do you consider that there are better safeguards under the proposed system?

Lord Judge: I think that pre-authorisation is something Parliament needs to look at across the board—but I would, wouldn't I, because I am convinced about our own little bit? If you do that, the papers come through to a commissioner, who knows what the law is, knows what he—or she, but we do not actually have any females—is looking for. If it is not good enough, if it is an urgent or relatively urgent thing, he speaks to the authorising officer, saying, "This is not good enough. Tell me more about this" or, "I am worried about the possibility that this suspect's wife is going to have her life intruded on". If satisfied—and usually you are, because they do not come unless they have a good case—then it is authorised. Then you inspect at the other end and you go through them.

I will add this, which I did not mention when I made my opening statement. From time to time, my inspectors will tell me that they are very worried about the commissioner having given an authorisation. They are not just examining the way the police are doing their work; they are a form of check that the commissioners are applying the law. Of course, it does not happen very often, but that is part of the process and I welcome it. If there is a case where I think the commissioner was wrong to make the authorisation, then I see him and say, "I think this was wrong" or whatever.

Provided that you, as the citizen, are satisfied that, before people can come intruding in your life, a decision has been made by somebody independent of those who are going to do the intrusion, and there is a system for inspecting afterwards, at random, what the various bodies have been doing, that is a pretty good form of safeguard. In my experience—again limited—I do not see cases where people or authorities are applying unless they have good grounds for doing so, because they know they will be refused.

Q50 **Lord Strasburger:** My questions are for Ms Cavan. I would like to start by congratulating you on the transparency of your reports and your engagement with the public through Twitter. I wonder if Mr McDonald's concerns about systemic difficulties and unwarranted activities would be allayed by the new commissioner being able to initiate inquiries on his or her own initiative, and perhaps even unannounced inspections. That is my first question.

Jo Cavan: On that note, we recently published a wish-list of some of the ways we feel the oversight provisions need to be strengthened. In one respect, the ability and mandate of the new commission to launch inquiries or investigations, we feel, could be further strengthened. We also feel that access to technical systems could be more explicit in the clauses. At the moment, the drafting is outdated: it refers to providing the commissioner with information or documents, whereas these days we are generally not looking at paper. When our inspectors go in, they have full access to the technical systems; they run query-based searches and look for compliance issues at scale, which is really important when you are dealing with these bulk collections. We think the oversight provisions and the clauses concerning technical system access and the ability to launch inquiries and investigations could be strengthened further.

Lord Strasburger: Lord Chair, would it be appropriate to invite Ms Cavan to put her views on how that might be strengthened to us in writing?

The Chairman: I am sure that would be fine.

Lord Strasburger: My second question is: how do you think we should strengthen oversight of international co-operation between Five Eyes intelligence agencies?

Jo Cavan: There are some additional safeguards in the IP Bill for the sharing of intelligence with overseas agencies. These matters have been significantly debated during some of the recent Investigatory Powers Tribunal cases. As a result of further disclosures made in those cases by the Government, the safeguards have been published and they are now in an amended code of practice. Certainly, that is an area we are looking at during our inspections and audits.

Sir Stanley Burnton: The fact we can interrogate the computer records of the authority whose activities we are auditing reduces the need for unannounced visits, because we have access to the raw data.

Q51 **Victoria Atkins:** Following on from Lord Judge's very helpful analysis of the oversight and review process, there is one angle that I am not sure the Committee has heard about yet, which is what happens at trial. Where an investigation results in a suspect being charged and a prosecution being brought, could you help us, please, with the duties on the prosecuting lawyer and prosecuting counsel to ensure that any warrants that may have been used during the course of that investigation were conducted properly, and the professional obligations on them as a reviewing process, in addition to all the reviewing processes you have already described?

Lord Judge: When everything has worked as it should have, and there has been no breach and no subsequent concern, that simply goes through. There is no disclosure. But, where there has been any breach—and, as Sir Mark pointed out, there are self-reporting breaches

as well as discovered breaches—it comes to me, and it is axiomatic that the first thing I do, having decided what should happen about the breach, is to say all the papers must now be retained and disclosed to the Crown Prosecution Service, in the event of a prosecution, for onward disclosure as seen fit. That is up to the prosecutor. That material, I am sure, would then go to counsel for the defence, who would then decide whether to make an application or not.

The other feature, which has been underlined by a recent decision in the Divisional Court called Chatwani, is that there is an obligation—it is obvious that there is, but the court has said so—on the person making the application to tell the whole truth. In other words, you set out the points you say are favourable to the application you are making and the authorisation you are seeking, but you also have to add the bits that do not fit. Chatwani was a case where what was going on was not properly disclosed and the Divisional Court said, "Quite obviously, you cannot work on the basis that the whole story is not told". Failure to tell the whole story would itself constitute a breach, which would then have this system fall into place: retain it, keep it, disclose it if there is a prosecution. Of course, often there is not a prosecution, which raises a different problem, but if there is that is how it is done.

Victoria Atkins: In addition to the many sets of eyes in your organisations, there is also, if a case comes to court, the extra review conducted by lawyers and counsel to ensure that processes have been applied properly.

Lord Judge: Yes.

Q52 **Baroness Browning:** You heard me ask Sir Mark about training. I wonder what training you feel might be necessary for the new judicial commissioners.

Lord Judge: Rather like Sir Mark, what you are doing is making a judgment. This is what, if you are a former judge, you have been doing for however many years you have been doing it. You have been making decisions like this day in, day out. The questions are very simple: is this necessary? Where is the evidence? Yes, on this evidence, it is necessary. Is this proportionate? I must bear this in mind and that in mind, and that in mind. On this evidence, that is proportionate. Hang on, there is a bit of this that might involve the suspect having had conversations with his, for the sake of argument, doctor. You have to be careful there. I mentioned earlier an intrusive surveillance into the family car that is being driven by the wife. Nobody suspects her of anything, so you cannot have that; it is not proportionate.

That is all you are doing. You are making a judicial judgment, which is what you have spent your whole career doing. I am not saying you are infallible, and I made the point a few minutes ago in relation to my commissioners: when they get it wrong, my inspectors will tell me. But you do not need special training for that. What happened to me is, in effect, I went and shadowed my predecessor. I went out on inspections to see what my inspectors did and how they went about it, and to see that they were doing the job the way I wanted them to do it. I go out with my commissioners. We meet regularly and discuss the problems that are current. That is the training, and then you take over the job.

Baroness Browning: With the advance of technology and things moving on so quickly, particularly once this is in one collective body, could the choice of methodology in the application that comes before you be something you question—whether this route is going to be used or that route? Does that not require some technical knowledge on the part of the person making the decision?

Lord Judge: Not really, because, for necessity, that does not arise. You do not need to know whether the nature of the intrusion is a probe that is one inch long or six inches long; you need to know whether there is going to be a probe. Of course, I have overlooked this. I spent time, two days ago, sitting in the National Crime Agency, being lectured to about how some of the worst aspects of child pornography being transmitted around the world are dealt with. We do try to keep up with that.

But, no, you are making a judgment. In the new system, I have no doubt—and I disagree with Sir Mark here—that there should be one or two people with serious expertise in technology. I also think there should be a legal adviser. The law is extremely complex. RIPA is a dreadful piece of legislation. I say that with some strength of feeling, having had to try to understand it. Why do judges need a legal adviser? For that reason: to say it could be any one of 17 possible interpretations, rather than the five you thought you had. More importantly, in this system, from time to time you need advice. That is what I would like to happen, but then I envisage this as rather different from the bits and pieces you are seeing put together before you today.

Q53 **Lord Hart of Chilton:** You heard us discuss with Sir Mark the question of the judicial review principles that underlie the judge's oversight. I wondered if any of you would like to comment further on what he said. We were exploring whether it is right to call it a real double lock system. Are there any points you would make, further to the points made by Sir Mark?

Sir Stanley Burnton: Judicial review is not simply a question of looking at process. In the context we are discussing, the commissioner has to look at necessity and proportionality. The degree to which judicial review is imposed as a test and the stringency of the test depend very much on the context, the facts of the individual case and the consequences of the administrative or governmental decision in question. In the context we are discussing here, it is not unfair to describe the process as a double lock.

Lord Judge: That is rather my view. My only hesitation, which is a lawyerly one but not totally without some force, is in using the words "judicial review" as a description of the test that has to be applied by the judicial officer. Judicial review used to be Wednesbury unreasonable mad. We would call it Wednesbury unreasonable, meaning only an idiot could have reached this decision. Nowadays, judicial review is less stringent than that: "He is not an idiot, but it is a really stupid decision". That is not quite the same. "I am not sure many people would have reached this decision" is another test. We need to be slightly careful.

If you are talking about the Home Secretary, and I think you are, I have a separate point. There is a difference between national security warrants and ordinary criminal warrants. What we do should be the system for ordinary criminal warrants: an authorisation in advance. That is a double lock. National security is rather different. The Home Secretary has the most amazing responsibilities in relation to that. Judges second-guessing is simply

inappropriate. You have to have a stringent judicial review test. I am now coming back to what Sir Stanley said. You know you are dealing with national security; you know somebody might be planting a bomb. You are going to be very cautious about interfering and saying, "This man or woman, who is the Secretary of State, is daft". So I think the double lock system will work pretty well.

Sir Stanley Burnton: You can forget about Wednesbury unreasonableness in this context. Interestingly, proportionality and necessity are tests that we have imported from Europe, and the proponents of the Bill are clearly happy to adopt them in this context.

Q54 **Matt Warman:** As a still fairly new Member of Parliament, it struck me, observing the procedures of Parliament, that, if you have some pretty crazy procedures around for long enough, they become lauded as institutions. You described a pretty crazy set-up in your opening remarks, but does it not function as a sort of quadruple lock on what we have already, if you are constantly going back to ask for re-authorisation? I wonder what we are going to lose by streamlining it, if anything.

Lord Judge: I am sorry, I must have been unclear. They are not re-authorisations. Each one is a fresh authorisation by a different body. Sometimes the body will not even know what the earlier authorisation was. It is not a quadruple lock at all. Each is an individual one.

Matt Warman: So you do not see any strength from having three different people.

Lord Judge: No. I see potential for confusion. A much more coherent system would enable the same commissioner to look at one case. "This is the case of Snooks. This is the drugs ring. Right, the undercover officer has gone in. Here he wants this. Does the authorising officer think this is appropriate? Yes", and so on. The whole thing can be kept, in effect, under one person's eyes. It is much more proportionate. Sorry I was not clear enough. They are separate organisations.

Matt Warman: The argument that has been put is: at the moment, we have three commissioners, and, if one person makes a mistake, who is checking up? You would not accept any of that.

Lord Judge: People make mistakes, certainly, but we are all independent organisations. We talk; we discuss problems together, but we operate completely differently. It is not a system with the three sections of this keeping an eye on each other. We do not.

Q55 **Lord Butler of Brockwell:** When we took evidence from Home Office witnesses last week, they introduced a new concept, new to me anyway, of rationality. We asked whether reasonableness would be a test, and the witness seemed to dissent rather. He made a distinction between rationality and reasonableness. Is that a distinction you recognise?

Sir Stanley Burnton: The Wednesbury test is a rationality test: that no sensible administrator or executive correctly applying the law could have reached this decision. It is not a very stringent test; it is only in extreme cases that you are able to say something is Wednesbury unreasonable, whereas proportionality and necessity are more stringent.

Lord Butler of Brockwell: You are saying that there is no great distinction between reasonableness and rationality.

Sir Stanley Burnton: I am.

Lord Judge: I would not have noted any difference between them. I would not have argued the point with you. If you had said "Is it reasonable?", I would not have said, "It has to be rational".

Q56 **Stuart C McDonald:** I have a rather more mundane question about money, I am afraid. The impact assessment suggests that the new oversight and authorisation regime should cost around £150 million over 10 years. Would you regard that as realistic? If you do not feel able to answer that particular question, would you say that you have had sufficient resources to carry out your jobs fully, or are there other things you would have liked to do that you have been constrained in?

Lord Judge: I could give you a list of my complaints.

Stuart C McDonald: Please do.

Lord Judge: Our technology is, for obvious reasons, supposed to be secure. Our Brexit system—I am so sorry; I have something else on my mind—our BRENT system is hopeless, so we want it improved. We wait too long for new appointments to happen, and so on and so forth. Parliament has to decide how much it is going to spend on protecting the citizen from the threats of crime and terrorism, and how much it is going to spend on ensuring that those who should not be being surveyed in any way at all are protected from it. If you go down this route, you will have to have—I would strongly recommend if I were asked, so I will tell you anyway—a location separate from the Home Office, and people working there who are not drifting in and out of the Home Office. The perception of independence is strengthened by going to a separate place.

I mean no discourtesy; our rooms are pretty cramped. You are going to have a big system. If you have the same number of commissioners I have, which is six plus me plus three assistant commissioners, that is ten before you start. If Parliament enacts a system in which there is authorisation for everything in advance, it is going to take a lot more people. It will cost a lot more. We can either do it on the cheap or spend more money. We are in times of great financial stringency. I am sorry, but this is really not for me to say. I might say it in a different role, but not here. Yes, it will cost a lot more.

Sir Stanley Burnton: I am not an accountant and I cannot give you a figure. My impression is that in order properly to run the system, there are going to be something like eight judicial commissioners, which is quite a lot of staff. They must be backed up with appropriate staff, with the kind of skills my office now has but more widely available. There will be more inspectors, who must be appropriately qualified. You are looking at significant sums of money.

Incidentally, on a question that Sir Mark was asked, it ought to be the chief commissioner who determines what staffing and resources are needed. He must, of course, approach the Treasury and agree a budget, but it seems to me to be inappropriate for the person who is being monitored in a sense to be the person who decides on the resourcing of the office. Indeed, internationally, one increasingly finds that judicial bodies are not subject to a

Ministry of Justice, so far as resourcing is concerned. It is the judiciary that determines the resources it requires, subject to Treasury agreement.

Lord Judge: I entirely agree with that. The idea that judges will be looking at the Home Secretary's decisions and saying, "We do not think that is right", and then going cap in hand to that same Minister is not a sufficient separation.

Stuart C McDonald: That is helpful, thank you.

Q57 **Lord Henley:** I asked Sir Mark earlier about cost. This takes me on from Stuart's questions. Are you saying that under the new arrangements you should, almost as the universities used to in the past, negotiate directly with the Treasury without any intermediary?

Lord Judge: That would be my view. I make this clear: I am not seeking appointment to be the high panjandrum for this. A direct communication between the Treasury and the Commissioner is the way to do it.

Sir Stanley Burnton: As a matter of principle.

Lord Henley: Is that because your independence would be undermined if you had to go through the Secretary of State?

Sir Stanley Burnton: The appearance of independence is undermined if one has to go through the Minister whose work one is supervising.

Lord Henley: I ask that purely because I remember, back in the long, distant past, that that is how university funding used to be done when universities were independent. It is no longer the case; there is a department that looks after universities. That might be the way forward.

Lord Judge: In the context of the way the judiciary works, there has been coming and going about this, but I used to agree a budget or not agree a budget. I also had the power, which I never exercised, not only to write and say, "I do not agree it", but to say, "I am going public and this will not do". You need some kind of arrangement like that. We are both in the same place. If we are going to supervise the Home Secretary, we must not be answerable to him or her for the money.

Q58 **Lord Strasburger:** Would you be attracted to the system that exists in New Zealand, where the people in your position have a fixed percentage of the spend on intelligence and policing, and the decision is taken out of politicians' hands?

Lord Judge: The decision as to money?

Lord Strasburger: Yes.

Lord Judge: Ultimately, the Government have to find the money, so there has to be a discussion with somebody who represents the Government. Therefore, that is why we both say the Treasury.

Sir Stanley Burnton: I think I would need notice of that question.

Jo Cavan: If we went to that type of model, our percentage would no doubt be significantly lower than the percentage in New Zealand, because of the larger scale of our intelligence agencies, in particular the bulk collection we do, in comparison to New Zealand. Anyway, I do not necessarily think it is a bad model. I would say that the legal mandate and oversight provisions the New Zealand inspector general has are far more explicit and comprehensive than the ones in this Bill.

One of our points on the clauses around oversight is that they relate only to judicial commissioners; they do not relate to the commission. If we are going to create this world-leading oversight commission, it is important that the commission is explicitly referenced and the legal mandate, powers and functions are comprehensively covered.

Lord Strasburger: For the second time, I will say something about judicial review. I asked the Home Office on Monday why the words "judicial review" were in there, and they could not really tell us. What would be the effect, do you think, if they were struck out? Would the Bill be better for it, or worse?

Lord Judge: Parliament has to decide what function the judge is to exercise. Judicial review is a well-known series of principles, even though occasionally you hear it expressed in different ways. As I said a few minutes ago, in terms of national security, the idea of the judge in effect making the decision simply cannot arise. If a bomb goes off in London tonight, it will be the Home Secretary who will be down there. It will be she who has to answer to the House about what has gone on; it will not be the judge. We have to be careful to remember that there is a political responsibility, which is in the hands of the Minister, and we cannot dilute that.

Sir Stanley Burnton: If I remember rightly, the legislation on control orders, which are orders short of imprisonment to control people who are suspected to be terrorists, also requires the judge to apply a judicial review test. In practice, of course, in SIAC, the judge hears, often in secret, the evidence that is available to show that someone is a security threat. He applies quite a stringent test, because he has the information and knows whether there is something justifying imposing a control order. The legislation has changed, but it is not dissimilar.

Q59 **Bishop of Chester:** The fear in some quarters is that this new system will end up with rubber-stamping, that it will not be sufficiently independent. That is the fear abroad in some quarters. I am trying to imagine life in the increasing digital swirl in the years to come, with the exponential growth in communications and means of communication. How can we get some feeling of control and exercise oversight, and not simply be carried along in the tide? The threats in the 21st century will probably increase as well. Can you give us some idea as to how this double lock, this independent supervision, will work in practice?

Lord Judge: I hope I am not being discourteous. It is very easy to drum up anxieties. I am just as worried about criminals being able to get hold of information as I am about any of the authorities. We concentrate on the authorities. I do not know what is going on in this room even as we speak, but the technology available to serious criminals is, at the very least, as good as is available to law enforcement people. You trust your judiciary to make decisions against the state when it is appropriate to do so. I do not think anybody suggests that the judiciary nowadays is less independent than it was. In many ways, it is more so.

You have men and women who have exercised these functions all their professional lives, first at the bar or as solicitors, then as judges. They are men and women of proven experience and quality. You just have to work on the basis that you should trust them.

Bishop of Chester: Would it be better for perception, if nothing else, if the appointment of the commissioners was not made by the Executive. Just as you made those comments earlier about having clear blue water between the Home Office and this, would it be better to involve an agency more independent than the Executive?

Lord Judge: It is the Prime Minister's appointment. The Queen appoints the Lord Chief Justice, but that is on the recommendation of the Prime Minister. I do not suppose the Prime Minister spends a lot of time deciding what he is going to recommend to Her Majesty. There is, in the case of the judges, a Judicial Appointments Commission. I would not recommend that for these appointments. Apart from anything else, they have far too much to do and it takes a very long time.

For the very last commissioner who was appointed to my team—and this you could consider—a senior serving judge and a member of the Judicial Appointments Commission sat together, with my predecessor as an observer, and they chose whom it should be, and the appointment was then made. That is a perfectly sensible system. It is only theoretical that the Prime Minister has anything to do with it. It is very nice for me to be appointed by the Prime Minister, but I honestly do not suppose anything more.

Sir Stanley Burnton: By prescription, the commissioners are going to be either actual serving judges or former judges, and so one has to bear in mind that they will have been independently appointed, initially. Whether they will be full-time judges working part time as commissioners or are expected to be full-time High Court judges seconded to the commission, the Bill does not make clear. We probably both have concerns about the ability of the existing High Court to have people seconded to a different function, given that the High Court itself is under pressure.

Jo Cavan: Before we move on, I wanted to talk about the end-to-end process, because a lot of the debate has been focused purely on the double lock and the authorisation process in the first instance. Yes, that is crucial, but what is equally crucial is the post-facto audit functions, which look at the process from end to end. We carry out over 200 inspections a year and make over 800 recommendations to improve systems and procedures in compliance.

The inspectors, during their inspections, are looking at post-authorisation: was the actual intrusion foreseen at the time the warrant or authorisation was given?; has the conduct become disproportionate because the level of intrusion was not anticipated? They are looking at how the material that has been gathered has been used. Has it been used in accordance with the purpose that was set out in the warrant? They are looking at the retention, storage and destruction procedures for that material. They are looking at whether any errors or breaches occurred as a result of the conduct. All those post-authorisation functions are critical to ensure that you are overseeing and auditing the end-to-end process. That is where the modification and ongoing review of these provisions come in.

Sir Stanley Burnton: The reviewer will also look at the duration of the warrant and may go to the public authority concerned and say, "How is it that this warrant has been renewed twice? What evidence have you been gaining from it? Was there any justification for its continuation for such a long period?'

Q60 **Mr David Hanson:** In relation to Clause 176, which establishes the budget, as we have discussed previously, are you therefore suggesting to the Committee that we should consider recommending a rewrite of that clause that separates completely the funding from the Secretary of State, not just in terms of the effective micromanagement that the clause could imply, although in practice it probably will not, but in terms of the principle that the Treasury should be the lead department that you directly negotiate with?

Lord Judge: If we retain the present Bill in relation to judicial oversight of the Home Secretary, yes, unequivocally.

Mr David Hanson: I have a second point. Lord Judge, I noticed you made the point that it is very nice to be appointed by the Prime Minister, but you are sure he does not take much interest in it. I suspect, as many people in the past, should you be a troublesome priest, he may take some interest in your reappointment. I am wondering, given what the Lord Bishop has said, whether or not consideration should be given to independent appointment, rather than direct ministerial appointment, into the oversight role, given that oversight role?

Lord Judge: If we envisage that, 20 years from now, the Prime Minister of the day decided that he or she was not going to re-appoint somebody, and had no good grounds for doing so save that he or she did not like the colour of their face, or whatever it might be, there would be an absolute scandal. I really do not think Prime Ministers would want to get embroiled in that sort of thing.

We have to be careful about public perception, if you do not mind me saying so. Most members of the public, I suspect, want to know that those of us who have responsibilities in this field are seeing that the job is done efficiently, ie to protect them, and fairly, to protect their own rights. That is what they want. I do not think that they are going to be terribly fussed, largely, about whether the Prime Minister's name goes on the appointment, or whether it is that of the Speaker of the House of Commons or the Lord Speaker. One has to be careful. That is my view about it. If I were in charge and, the Prime Minister failed to re-appoint somebody and I thought this was the reason, I would go and see the Prime Minister and tell him, "I will go public about this".

The Chairman: Thank you very much indeed. It was a fascinating session and we are grateful to all of you for coming along. You have given us very interesting stuff to chew over, to say the very least. Thank you very much indeed.

Lord Judge: Thank you.

Sir Bruce Robertson, New Zealand Commissioner of Security Warrants (QQ 250-258)

Evidence heard in public Questions 250-258

Oral Evidence

Taken before the Joint Committee

on Wednesday 6 January 2016

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins, Suella Fernandes MP, David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Bishop of Chester, Lord Hart of Chilton, and Lord Strasburger.

Witness: **Sir Bruce Robertson**, New Zealand Commissioner of Security Warrants, gave evidence.

Q250 **The Chairman:** Good evening, Sir Bruce.

Sir Bruce Robertson: Good evening.

The Chairman: Are we all here? This is the first time I have conducted a meeting with someone who is more than 10,000 miles away but we are very grateful to you, not least because of the unearthly time it is in New Zealand. Our deepest thanks to you. As you know, this is a huge Bill that Parliament here in the United Kingdom is going through. We have been set up to look at the Bill for pre-legislative scrutiny. We are composed of Members of the House of Lords and the House of Commons. We are particularly interested in talking to you about your experiences, and I repeat that we are very grateful indeed that we have this chance to do so.

I will open with a general question which will give you the chance, if you wish, to make some opening statements that you think might be useful to the Committee. Obviously we are looking at the comparative roles of the Investigatory Powers Commission and yourself. How does the role of our proposed new Investigatory Powers Commission compare to the job that you have been doing?

Sir Bruce Robertson: I think the fundamental difference between what is proposed and the task that I undertake is that my role is restricted entirely to the issue of granting the warrant in the first place. I have no supervisory or auditing role beyond that point. We have a split between the power to allow an interception warrant to be granted and the supervision of what continues thereafter. When there is a desire on the part of either the security service or the GCSB to get authorisation, they make an application to the relevant Minister but the Act provides that the relevant Minister can grant an authorisation only if I concur with the granting of it. It is an entirely dual operation. From my experience of three years and the experience of my predecessor, who was in office for almost 14 years, this appears to provide a sensible and operational joint protective measure. Parliament has made clear the basis on which authorisation can be granted. Procedures and protocols are in place which

ensure that this is done only when it is necessary, reasonable and proportionate and where there are no alternatives available.

When, as a judge, I was involved in the issuing of warrants to police officers—as a High Court judge my involvement was restricted to drug cases and criminal conspiracy—the issue was entirely about law enforcement. There was no executive involvement or activity at all. In the area of national security, there are, of course, two sets of issues that need consideration. One is whether what is sought is lawful. The second, which is the Executive's decision, is whether or not it is an appropriate course of action to be adopted.

I have the time, and I take the time, to investigate a proposal or a request in some considerable detail. As I said in some of the earlier material I submitted, when there is an application I receive an indication that this is afoot and I go to the premises and first of all read the file. The file, as is inevitable in this sort of area, will be voluminous but I have the time to do that. I have the time to analyse it. I have the time to dissect it. What is as important as anything is that I have the opportunity to actually meet the people involved with the application. When the formal steps are taken, the director will be there, but at the earlier stage I meet the people, first, in the legal division and, secondly, those who are moving on the ground, to discuss what is sought and why it is necessary, why it is proportionate and what is available. It is not uncommon for there to be some tweaking or tightening at that less formal stage. Then I meet the Minister in person to discuss our joint responsibilities in respect of that issue.

It is important, however, that once that has been done and a warrant has been granted and issued, I am not involved in the auditing process of whether it has been properly put into effect and the operations are appropriate. That is part of the remit of the Inspector-General of Security and Intelligence. She has a substantial staff. I do not have a staff; we are dealing with a relatively small country. Of course, the difference between our situation and yours is that my involvement is entirely in the security area. I do not have any involvement in other areas of law enforcement.

The Chairman: Thank you very much. Can I ask you about the very urgent cases that from time to time come up? In the system that you have just described, how do you operate when an extremely urgent case appears before you?

Sir Bruce Robertson: I put on my running shoes and I get myself to the Minister's office. There is inevitably a period of some hours. In the cases that are truly urgent and need something done in a great hurry, I will be contacted at the time that they are trying to set up an application time with the Minister. Sometimes the reading and briefing that I do will be truncated and might occur in a foyer or in the lobby of the Minister's office. I have been pulled out of dinner. I have been pulled out of my bed. But it is not a frequent thing, at least in New Zealand. In the overwhelming number of cases, the two services operate on the basis of having a little time. It is not impossible to get a retired person, when they are required, to be available as quickly as the Minister would need.

The Chairman: Thank you very much. That is very clear.

Q251 Mr David Hanson: Good afternoon. You mentioned in your submission that your predecessor held the post for 14 years. The proposal in the Bill is for the position to be held

on a three-year contract. Do you see any advantages or disadvantages in that length of appointment?

Sir Bruce Robertson: Sorry, I was perhaps less clear than I should have been. The appointment is for three years, but my predecessor was reappointed on a number of occasions. My appointment is for three years, but I can be reappointed. It makes a lot of sense to have an opportunity to reassess because one has the normal powers and protections that a judge would have. Removal is by grace of Parliament. Under our system in which the appointment is made by the Governor-General on the advice on the Prime Minister after consultation with the Leader of the Opposition, it is sensible that there should be an opportunity for periodic review.

Mr David Hanson: The method of appointment proposed in the Bill in the United Kingdom does not involve the Opposition and is a prime ministerial appointment in consultation with the devolved Administrations in Scotland and Northern Ireland. Do you think that the New Zealand model with a Governor-General appointment on recommendation with consultation with the Leader of the Opposition is just different or is it better or potentially worse than the current proposal?

Sir Bruce Robertson: It seems to me that there is a strong argument for the most independent position that can be created to be created. That is done in New Zealand by appointment by the Governor-General. Because of the sensitivity of this area and the importance of public confidence in what is done, the requirement to consult the Opposition before the recommendation is made is worthwhile. Much of this is about the perception of whether there is an independent, objective inquiry going on by a person who is clearly independent of the Government of the day. My predecessor was obviously appointed by different Governments of different hues over the years. He was simply seen as a person of enormous integrity who had the ability to do the job. It was in no way a "political appointment".

Q252 **Lord Hart of Chilton:** Good evening. As you have been a judge for more than 18 years, independence runs through you as a sort of DNA characteristic.

Sir Bruce Robertson: I hope so.

Lord Hart of Chilton: How do you maintain that independence from Ministers? Does that mean that you foreswear all cocktail parties and all dinners and do not go to rugby internationals where they might be? How do you go about it?

Sir Bruce Robertson: None of the matters that you have alluded to would have interfered with my independence in the task I was carrying out. In the 28 years I was a judge, I had no difficulty in reaching a view different from that held by the Government or any other litigant with whom I was involved. My task now I see as simply analysing and assisting with the evidence. The great attribute which an experienced judge ought to bring to the task is the ability to weigh and assess and sometimes to put a fairly weary eye across a proposal. I do not think any of us should ignore the fact that in this area of public life, as in others, there will be very committed views which are genuinely held which do not always stand up to the strictest scrutiny. In speaking with quite senior officers who, let us say, have reached a view that there is no alternative to what they propose, they can be challenged, questioned and

the like. When it comes to the Minister, when I was appointed to the position in New Zealand the relevant Minister was the Prime Minister and I was not overawed by that in any way, nor am I overawed by the fact that the Minister at the moment is the Attorney-General and Minister for Security. Both the people I have dealt with have been capable of fairly rigorous debate with me. As a judge obviously you have to maintain, for public confidence, a degree of independence, but that is the way it is in the life of a judge, so there is really nothing different about that.

Lord Hart of Chilton: Thank you. Does the draft Bill include sufficient safeguards to uphold this important dimension of the independence of the commissioner's role?

Sir Bruce Robertson: As a matter of policy, the ability to be independent, objective and effective is enhanced and embraced if the input is prior to the issuing of the warrant. As I perceive what is proposed under your draft Bill, a person in my position would come in after the event. That becomes a matter about the standard of review and the manner in which that review occurs. It is a much more powerful, potent and effective check if the person in my role is involved in the initial granting of the warrant before anything is being challenged.

No matter what words you put around it, as soon as you get a challenge to something which has already occurred, all sorts of questions arise about whether it was a permissible activity and whether it should be altered. That is the issue in judicial review in the normal court system. The New Zealand arrangement allows independent involvement before the warrant is granted so that the question of whether what is proposed is lawful in its widest sense is part of the initial assessment, not an after-the-event review. There is real advantage in what we do.

Lord Hart of Chilton: Does that mean that you, in considering and reviewing before the event, are able to substitute your opinion for that of the Minister?

Sir Bruce Robertson: The Act says that we each must agree about what can occur. As a matter of common sense and the separation of power, it would not be for me to become involved in issues of high policy providing they are matters which are legally able to be undertaken. So although the Act does not categorise the area in which each of us works, it is inevitable that we bring different skills, experience and assessment to the task. In New Zealand, our Parliament decided that these two matters were of equal importance and that both should be given proper scope and operation before the warrant is granted. If what was being asked for was lawful and proper in the terms that I have talked about previously, then it would seem to me a very unusual situation if I were to endeavour to force my view on an issue of high policy on someone else. But let me say that it is not a matter that has created issues. I have at times raised with a Minister my concerns about a proposal. We have been able to talk it through and have reached a common view, but that is not a commonplace problem.

Q253 **Lord Strasburger:** Good morning, Sir Bruce. Still on the subject of independence, how is your budget and the budgets of other intelligence oversight bodies in New Zealand set? Are they set independently of the Government?

Sir Bruce Robertson: They go before a Select Committee of Parliament which has responsibility, and a local budget is granted to them. It is not a matter in which I have any particular involvement because my activity is restricted to a relatively narrow area, which, at least in my judgment, requires my personal involvement and intervention. I have no need for a budget of any consequence or size for myself. The issue of how the Secretary-General, who does have a large staff, operates is a quite separate one on which I shall not comment.

Q254 **Suella Fernandes:** Good morning. I would like to look a little more at the comparison between ministerial authorisation and judicial authorisation of the warrants. As you know, in this country it has traditionally been the Home Secretary or Ministers who have the power to issue these, in contrast to the situation you are setting out. To be clear, when you are considering your decision, you apply a legal test. That is right, is it not?

Sir Bruce Robertson: The Act does not restrict in that way. I am saying that it is a matter of operational activity. That is the real strength which I bring to the activity. In ensuring this careful check and balance, it does not appear to be part of my role to intrude into other areas to the extent that what is proposed is lawful and therefore available, but perhaps in my personal view not as prudent as it might be. I would not hesitate to express a view or to question a matter, but I am doubtful that in that narrow area I would be likely to want to force my view on another. It is difficult for me to see how that would be appropriate, but my experience is that that is not a decision I have ever been forced to take.

Suella Fernandes: So you apply a narrower legal test that is more limited in scope—would you not agree?—than a potential political approach, which would include factors such as high policy, as you describe it, or a sense of the national security issues, the nature of the threat, or even the additional factors of diplomatic or reputational risks to the issue of a warrant. They are not necessarily relevant factors in your decision-making process, are they?

Sir Bruce Robertson: The Act does not say that I am excluded from consideration in that area. The Act says that together we will grant a warrant and make an authorisation. I am simply saying that, as a matter of practical reality, in my assessment of diplomatic repercussions, high policy and that sort of thing, I would not seek to hold the line in the way that I would with regard to whether a measure was actually lawful. The question of how a person exercises authority is partly a question of serious judgment. There are competing interests which have to be dealt with. Provided that the alternatives are lawful, I do not see that it is my task to impose my personal assessment of a situation. But, as I say, I do not see why, as part of the overall process, I should not be involved in questioning or challenging to ensure that the requirement of legality is still being met.

Suella Fernandes: One last question. In terms of your decision-making, in the event of a mistake or some other error, what is the accountability that you have to meet? What is the appeal route and the scrutiny that you are held to?

Sir Bruce Robertson: The Inspector General, as part of her general remit, can look at issues around the granting of a warrant and can report on that, but my position is not one in which I am held out publicly to be questioned or assessed. This is the general process of auditing and supervising, and we are part of that process, but there is not an individual way in which

the commissioner, any more than the Minister, is called to stand up in the marketplace and explain what they did and why they did it.

Suella Fernandes: Although would you agree that, unlike a Minister, your role is less public—or, to put it another way, Ministers are elected and more public-facing, and therefore have an element of greater accountability?

Sir Bruce Robertson: In all my years as a judge, although I could not be called to account in the way that you are speaking of, I did not ever think that I was not accountable publicly. Certainly in the environment in which we live now, in your country and mine, judges are the subject of discussion by the public in a very general way, and no doubt could be in this situation. However, I accept that I am not held out in a way that a Minister can be because they are elected.

Q255 **The Chairman:** You have explained very clearly, Sir Bruce, that in your decision-making on this matter you concentrate on the legality, but that you are not restricted by legislation so to do. Would you occasionally take into account proportionality and necessity as well as legality?

Sir Bruce Robertson: Proportionality and necessity are part of legality. As I see it, the regime in my country and that proposed in yours require that proportionality, alternatives and reasonableness are all matters that go to the legality of what is proposed. That is why I do not see a hard line between the one and the other, and why it would not be practical to say that a person in my role is entitled to have a legal involvement. The two are inevitably intertwined. I am saying simply that when it comes down to a question of national security or high policy, my personal assessment should not be given undue or particular weight if the alternative proposed is otherwise a lawful alternative that is available.

The Chairman: Thank you very much. That is very clear.

Q256 **Dr Andrew Murrison:** Good morning, Sir Bruce. You paint a picture in New Zealand of a fairly collegiate approach to warrantry on national security matters. I suspect that that would not wash terribly well here, and certainly the draft Bill before us at the moment is not drafted in those terms. Indeed, it is quite specific: the judicial commissioner who is proposed here would be bound by the general rules of judicial review. What do you think about that? Do you think that a merits-based assessment by the judicial commissioner of the sort that you are describing would be more appropriate? Would you comment on what happens in New Zealand in the event that the collegiate approach that you have described breaks down and you disagree with the Minister or some subsequent Minister, or your successor disagrees with subsequent Ministers? Bluntly put, who wins, or is it a default position that the application fails?

Sir Bruce Robertson: My involvement at the stage at which I am involved is a much more potent force for providing protection for the general public. I have to say that in my term a total impasse has never arisen; we have been able to come to an accommodation and an agreement that was acceptable to both of us. Technically, the position is that if a commissioner were unable to agree to a course of action, a warrant could not be issued. There is no doubt about that. The position, which you describe as collegiate, I see simply as one in which two people, each with experience and total integrity, reach a view on the

available evidence. One of the important values that I can bring to the task is that there must be an evidential basis rather than a hunch or an emotive reaction of some sort. There needs to be some material that can be pointed to which justifies this degree of state intervention. When you come to look at the subsequent scrutiny by a judicial officer, it is inevitable that the paraphernalia around judicial review will emerge. That is a less potent force than when you have early involvement prior to the granting of the authorisation. What we are talking about is balancing competing interests, including the interests of people who cannot and will not know that the process is going on at all. What you decide is the extent to which you want to have a rigorous legal assessment before there is any authorisation. The subsequent activity, and the supervision and auditing that goes on, does not provide the same heightened level of protection that the New Zealand model can.

Q257 Stuart C McDonald: Sir Bruce, you have already pointed out that you have no supervisory or auditing role. That is very much in contrast to what is proposed in the Bill. Would the Bill be improved by including a similar split to the one in New Zealand?

Sir Bruce Robertson: The most that I could say is that the New Zealand system works. It enables an early involvement of the claim of legality. I would be uncomfortable about a position in which I was required to second-guess and reassess what I had already agreed to at an earlier stage. The division appears to me to be workable and to be strong in its principled approach.

Stuart C McDonald: That is very diplomatically put, thank you.

Sir Bruce Robertson: I do not know that I have a reputation for being diplomatic.

Q258 Matt Warman: To pick up on an earlier question, are there any circumstances to your knowledge where the time that it has taken you to get together with the Minister and have the conversation has held up the operational effectiveness that the security services might like?

Sir Bruce Robertson: Not to my knowledge. I suspect that sometimes the relevant people probably find it quicker and easier to keep me available in a spot than they do the Minister. I have been pulled out of a dinner and out of my bed, but I can operate less quickly and have fewer ongoing demands on my time than the senior Minister would have.

The Chairman: Sir Bruce, we are indebted to you for a very valuable session. The international comparison has been intriguing. Again, our apologies to you for it being so early in New Zealand, but this has been very important for our Committee's deliberations. Thank you.

Sir Bruce Robertson: Thank you so much. Good morning.

Professor Mark Ryan, Professor of Computer Security, School of Computer Science, University of Birmingham (QQ 76-93)

Evidence heard in public Questions 76-93

Oral Evidence

Taken before the Joint Committee

on Monday 7 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Bishop of Chester, Lord Henley, Lord Strasburger.

Witness: **Professor Mark Ryan**, Professor of Computer Security, School of Computer Science, University of Birmingham, gave evidence.

Q76 The Chairman: We extend a very warm welcome to our four guests this afternoon. We are very grateful to all of you for coming along on what is a hugely significant Bill that is going through Parliament—the Prime Minister called it the most important of this Session. Thank you very much indeed. As you probably know, the procedure is that I will kick off with a question or two, and then my colleagues will in turn ask you various questions on different aspects of the Bill that I think you find very interesting. If, when I ask a question of an individual, he wants to preface his remarks with a short statement, that is entirely up to him. I turn first to Dr Bernal. After you have answered, colleagues will be able to come in. What are your views on the draft Bill? Does it deliver the transparency on investigatory powers that you have particularly called for?

Dr Paul Bernal: Perhaps the best way to put it is that it goes part of the way. As far as I am concerned, it is good to see everything in one place, or almost everything—some bits are clearly missing—but for proper transparency we do not need just the Bill; we need the process to work properly as well. I would have said in my introductory remarks, had I made any, that the timetable makes it very difficult to get as much scrutiny as we would like; we have been called here very rapidly, and you have only a few weeks to do this. For transparency to work properly we have to have the chance and time to put our analysis into action. It is a bit difficult to do that.

One other thing I would say about transparency is that certain terms are used and expressed in a way that is not as clear as it could be. There are terms like "bulk powers" when we do not really know how bulky "bulk" is, if you see what I mean. For things like Internet connection records, it has taken some time, and we are still only part of the way there, to tease out what it really means. From that perspective, it is good to have it all in one place, but the process needs to be stronger. We need to make sure there is enough time to do it, and I am not sure you have as much of it in this Committee as you would like—perhaps later on there will be time—and we have to tease out some of the terms more accurately.

There is one other aspect. Some of the things in the Bill will become dependent on codes of practice and similar things that go with it. For transparency's sake, so that we understand what is going on, those codes of practice need to be put in a form that we can all see prior to the final passage of the Bill.

Q77 The Chairman: You have touched on the second question I was going to ask, so I will raise it now. You mentioned the codes of practice, which are hugely important in all this. What do you think the legal status of those codes might be?

Dr Paul Bernal: The legal status of the codes depends a little on how the final Bill turns out. From our perspective as legal academics, the key thing about codes of practice is not so much their legal status, which, depending on how it is set out, will be clear, but the extent to which they are also subject to the level of scrutiny and attention that the Bill itself is. It is easier to pass a code of practice through a small statutory instrument than to pass a whole Bill with full-scale scrutiny. We want to make sure that the codes of practice, which can be the critical part, get the same degree of scrutiny and attention both from people like us and from people like you.

The Chairman: With regard to the timetable, of course the issue that affects both this Committee and Parliament is, as you know, the sunset clause in the current legislation. Parliament has now laid down the amount of time we have. We certainly ensured that we gave ourselves extra and longer sessions, including in and around Christmas, and I am quite convinced that both Houses of Parliament will give it very thorough investigation, as indeed they should, but the point has been made. Does anybody else wish to speak on those issues?

Professor Sir David Omand: If I may make two remarks, the first is to stress the importance, in my opinion, of the Bill as the culmination of 500 years of history. It has taken 500 years to put the secret surveillance activities of the state under the rule of law. For centuries we had the royal prerogative being used in secret. Parliament passed the device of the secret vote but asked no questions. We had executive regulation in the last century, and for the past couple of decades we have had a patchwork of provisions in legislation, so all that secret activity was lawful but not understood. This Bill now places it under the rule of law; it will be comprehensible to the citizen. I cannot overestimate the importance of the Bill.

The second point is to agree strongly that it is in the codes of practice that the public will find it easiest to understand what is going on, rather than in the technicality of the Bill itself, so the codes are very important. Schedule 6 to the Bill sets out very clearly what the status of those codes will be. They will have to be presented to Parliament, along with the enabling statutory instrument.

The Chairman: Professor Anderson or Professor Ryan, are there any comments you would like to make at this stage before we move to other questions?

Professor Ross Anderson: I believe you will be asking me in due course about Internet connection records.

The Chairman: We will.

Professor Ross Anderson: It would be great if, in addition to having codes of practice, we had very much greater clarity on definitions. I will discuss Internet connection records, but there are other things that are not really defined at all, from the great concept of national security down to some rather technical things. I hope that clarification comes out during the Bill's passage.

The Chairman: You think such definitions should be on the face of the Bill.

Professor Ross Anderson: Yes.

The Chairman: Professor Ryan, are there any initial comments you would like to make to the Committee?

Professor Mark Ryan: Just on questions 1 and 2?

The Chairman: At this stage, yes, because there will be other more detailed questions, some of which will probably be directed to you personally as well, but at the beginning of the session would you like to make any general comments?

Professor Mark Ryan: The comment I would like to make about transparency is that this seems to be such an important area that the kind of oversight proposed is not enough. One would need more quantification of the sort of surveillance that takes place. Of course, I am aware that surveillance has to be done in secret, but I believe that the quantities of surveillance and the nature of surveillance can be disclosed to people without compromising the secrets of the surveillance activity. That seems to go more towards transparency and is much stronger than mere oversight, so I believe there should be more of that.

Q78 **Dr Andrew Murrison:** You have covered a huge amount of ground in about seven minutes. You hit the nail on the head in terms of definitions and the need to ensure that codes of practice and statutory instruments are sufficiently transparent and that scrutiny is of the utmost. I am interested to know how you think scrutiny and transparency can be improved other than through the normal process of laying statutory instruments before the House, because I sense from what you said that you feel that the Bill, which talks about SIs and codes of practice, is not sufficient in that respect.

Dr Paul Bernal: I would not say exactly that it is not sufficient. What I am interested in is getting as much scrutiny as we can. In order that we can understand the Bill we need to have the codes of practice at the same time, at least in draft form, so that they can be examined; frankly, to understand some of the powers in the Bill without a code of practice is very difficult, particularly on things like bulk powers and Internet connection records. We will talk a lot about Internet connection records later, but they are defined in such a way that it is unclear on the face of the Bill exactly what they will mean in practice.

Historically, not as much attention is paid to statutory instruments by the House. You do not spend as much time passing them as you do Bills; you do not have Committees scrutinising each of the statutory instruments at the same level of detail.

Dr Andrew Murrison: But it is worse than that, is it not? This is a very rapidly moving field, so you cannot reasonably lay all the codes of practice and anticipate all the SIs at this time, since 12 months down the line there may be yet more to come.

Dr Paul Bernal: Yes, and that is a fundamental problem with any kind of Bill in this area. I do not know whether there would be a mechanism to produce better scrutiny of the codes of practice, but attention should be drawn to the fact that this will be important as it continues. It needs constant attention, not just at the moment we pass the Bill.

The problem with the Regulation of Investigatory Powers Act was that, although it got a lot of attention at the time, the things that gradually built up to create the confusion—chaos is not quite fair—for people about the overall regime, and which stimulated the need for this Bill, were not sufficiently attended to over the years as things happened. We need to make sure that does not happen this time around.

Dr Andrew Murrison: Do you think a sunset clause would help? We are replacing one sunset clause with another. Is that inevitably where we are going to be led?

Dr Paul Bernal: Frankly, in this area you need sunset clauses in almost everything, because the technology moves and the behaviour of people changes. The overall situation changes. You need to be able to review these things on a regular basis, and a sunset clause is one of the best ways to ensure that happens.

Professor Ross Anderson: Last time around how we dealt with this was that, in the run-up to the passage of the Regulation of Investigatory Powers Bill through Parliament, a number of NGOs organised a series of conferences called Scrambling for Safety, and afterwards various statutory instruments were laid before the House. We are proposing to do the same again. The first Scrambling for Safety workshop is to be held at King's College London on 7 January from 1 pm to 5 pm, and all members are of course very cordially invited. We anticipate that it will be the first of a series that will enable engineers, lawyers, policymakers and others to dig into the meat of what is going on, exchange views and push the thing forward.

Q79 Suella Fernandes: Based on your expertise, would you set out briefly the nature and extent of the problem or threat we are facing when it comes to the use of this technology?

Professor Ross Anderson: The problem with the use of surveillance technology is that, if it is used in ways that do not have public support, it undermines the relationship of trust between citizens and the police, which has been the basis of policing in Britain for many years. Sudden revelations like Snowden are extraordinarily damaging because they show that the Government have been up to no good. Even though the Government may come up with complicated arguments about why bulk equipment interference was all right under Section 5 of ISA and so on, it is not the way to do things. There was a hearing in the Investigatory Powers Tribunal last week on that very issue.

There are other issues. The first is national leadership. If we go down the same route as China, Russia, Kazakhstan and Turkmenistan, rather than the route countries such as America and Germany have gone down, there is a risk that waverers, such as Brazil and India, will be tempted to follow in our wake. That could lead to a fragmented IInternet, with

extraordinarily severe damage for jobs, prosperity, international stability and, ultimately, the capability of GCHQ to do its mission, because if you end up with the IInternet being partitioned into a number of walled gardens, like the Chinese or Iranian ones, they will be very much less accessible to the intelligence agencies.

In addition, if the powers are abused, or seen as capable of being abused, there could be exceptionally serious damage to British industry. If people overseas come to the conclusion that, if they buy a security product from a British firm, it may have a GCHQ-mandated back door, they will not buy it; they will buy from a German firm instead. This is where the rubber hits the road when it comes to overreach in demanding surveillance powers.

Professor Sir David Omand: On the other hand, my advice to the Committee would be that this Bill contains the basis of the gold standard for Europe. This is how you get both security and privacy in respect of freedom of speech. The interplay of checks and balances and oversight regimes means that none of what Professor Anderson has described needs to happen. Of course, with a malign Government and agencies that flouted the law it would be possible to have abuses. I do not believe that either is likely, and certainly the provisions in the Bill allow this House to maintain very strict control of the Executive in its use of these powers.

Professor Ross Anderson: With the greatest respect, the reaction of America and Britain to the Snowden revelations has been somewhat different. In America people have rowed back in all branches of government. For example, President Obama has, simply by executive order, commanded the NSA to minimise the personal information of unaffected foreign nationals, like us. The legal branch has seen to it that, for example, national security letters, which used to be secret for ever, are now disclosed after three years, and Congress failed to renew provisions for the retention of American citizens' communications data. All branches of government have pushed back and sent a solid signal to the world that America cares about privacy and the proper regulation of its law enforcement and intelligence services. If the reaction from Britain is different, even if powers are not abused, it still sends a signal to the Brazils, Indias and, may I say it, the Kazakhstans. We do not really want that.

Q80 **Bishop of Chester:** A sunset clause is the nuclear option of legislation, but reading the Bill I am wondering how there is a process of inbuilt review, because the scene is changing so fast. There is a technical supervisory board bringing together stakeholders and so forth. Should there be an inbuilt power to renew the provision? That has been in some previous terrorist legislation. There has not been a formal sunset clause, but there has been a renewal motion. That would force Parliament to review what is happening, because for the legislation to continue there would have to be a renewal notice.

Professor Sir David Omand: Of course, it is Parliament's prerogative to put in such a provision. My experience in the public sector is that it should be done very sparingly, because it may turn out that at precisely the moment you have to legislate afresh, as with DRIPA, Parliament may not actually want to legislate afresh. One concern I had was whether the definitions in the Bill were sufficiently robust to deal with technical change. Having studied them, I am as confident as I can be that they avoid hostages to fortune, so your House will not discover in a couple of years' time that a different Bill is needed because the technology has moved on, but that will need to be examined by detailed scrutiny.

Q81 Shabana Mahmood: My first question is to Professor Anderson and then his colleagues. We have two competing narratives of the Bill: one that these are significant new powers and major changes, and the other that it is just codifying current provisions and bringing them more obviously and explicitly within the rule of law, as Sir David suggested. Professor Anderson, what is your view as to which of those narratives is more accurate?

Professor Ross Anderson: The Bill has been marketed as bringing in only one new power, namely Internet connection records, but it does many other things as well. For example, when the Regulation of Investigatory Powers Bill passed through this House and became an Act, one of the things we lobbied for and secured was the provision that if the agencies wished to command somebody to decrypt something, or hand over a cryptographic key, there should be special safeguards. The City of London did not want a rogue superintendent, perhaps in the pay of a criminal gang, to approach a 24 year-old assistant shift supervisor at a bank's data centre somewhere in east London and command him to hand over the bank's master signing key. Therefore, the provision was made that the production of a cryptographic key had to be demanded by a Chief Constable in writing and the letter had to be presented to a main board director of the bank. There are many provisions like that which appear to be swept away by this new legislation. Parliament must realise that the arguments are just as strong today as they were then; otherwise, how are you going to persuade international banks that London is a good place to do business? Some banks already had issues last time around.

My second comment is that a number of things that were previously done secretly were made public only in the run-up to this Bill, which enables the Bill team to say, "This is old stuff. We knew about it already". I refer members to the Investigatory Powers Tribunal hearing and the long arguments therein about whether an ISA Section 5 warrant could be used for bulk interception or only targeted interception. There are many technical aspects like that.

Thirdly, although the Internet connection record is ostensibly the new thing in the Bill, it actually gives very much greater powers than have been advertised; rather than just helping IP address resolution, it enables a policeman to say, for example, "We have these two bad people. Show us all the websites they both visited last month, and tell us the names and addresses of everybody else in the world who visited the same addresses". That is an extraordinarily powerful capability. It is the sort of thing that Internet service companies use to fight spammers, phishermen, click fraudsters and so on. Those of us who have worked in that field know how powerful it is and tend to be of the view that it should be classified along with intercept. If we are to have a special higher burden for intercept warrants, that higher burden should apply also to complex queries that are made on traffic data.

Shabana Mahmood: Have you done any analysis of powers advertised one way but which, as you suggest, lead to, say, five extra things? Have you made some sort of qualitative analysis to back up the examples you are helpfully giving us?

Professor Ross Anderson: The qualitative analysis basically comes from experience working at Google on sabbatical four years ago with the click fraud team. Knowing that such inquiries are extremely powerful, and talking to colleagues at Yahoo and Facebook recently, there is general concern that, if you allow people to make complex queries like that, it is up

at the level of a box of fancy tricks; it is not the sort of stuff you want to let an ordinary policeman do without supervision, because it can be used to do some very bad things.

Professor Sir David Omand: The Bill does not provide for ordinary policemen just to request that. There is a mechanism for a single point of contact and independent agreement before data can be acquired. I do not recognise either of the extreme cases Professor Anderson puts forward, but no doubt the Committee will need to investigate that further.

Dr Paul Bernal: If I may add something in response to that, there is something missing in the idea that these are either new powers or old powers. People's behaviour has changed fundamentally. The Internet, which was a medium used for communications—in the old-style idea of communications—is now used for almost everything else: shopping, dating, research and that kind of thing. The same power applied in a different situation gives a significantly higher level of intrusion than we have ever seen before. It is not like listening to phone calls, reading emails or things like that; it is like following people down the street while they shop, looking at the books they take out of the library and things like that. Without even changing the law, you are significantly changing and increasing the level of intrusion. It has lots of different implications, not just in terms of the balance of privacy and things like that but all the other rights we normally think of. Our expectations of privacy are different from those we had in the past. In a way, it comes down to the idea of how the law is going to change and how we need to take things into account. We need to take into account not only developments in technology but the way people's behaviour changes in relation to that technology; for me, in effect, that is the biggest increase in power. It is not that there is a new power built into the Bill, but because we use communications so much more extensively it is a much more intrusive thing to do any kind of Internet surveillance.

Professor Sir David Omand: That is why the Bill defines event data, Clause 193, in a conservative way, not taking modern metadata but imposing on the rather fuzzy reality some precise definitions, to minimise—it cannot be avoided completely—the kind of case Dr Bernal referred to. Inevitably, if you impose strict definitions on fuzzy reality, you will occasionally get hard cases. Those will exist in this world. As we know, the difference between dangerous driving and driving without due care and attention means that sometimes cases fall on the wrong side of the line, but the old adage that you do not make law by hard cases still applies. I commend to the Committee the way that the Bill has not expanded the definitions of communication data in defining event data.

Q82 Shabana Mahmood: That is helpful. You touched briefly in your previous answers on my final question, which is about future-proofing the Bill to take account of the pace of behavioural and technological change. We had evidence from officials from the OSCT. They were very bullish and confident that the changes in relation to Internet connection records in particular meant that it was sufficiently future-proofed. Could we have your comments on that?

Professor Ross Anderson: I have two main comments. The first is from the viewpoint of the long term—20 years out. We are simply asking the wrong question. The right question is: what does the police service look like in a modern technological society? Is it completely centralised? Does it go like Google? Do Ministers take the view that a chap sitting in Cheltenham can learn more about citizens in Leicester than a bobby on the beat in

Leicester? What sort of society does that become? This is a much broader conversation than just about who gets access to whose mobile phone location trace when.

The medium-term issue, which I think will become acute over a period of five to 10 years, is that the real problem is a diplomatic one. The real problem is about jurisdiction and how we get access to information in other countries, specifically America. America is where the world's data are kept. If they are kept in Finland or wherever because of cheap electricity, usually they are still controlled by a US company. There are some exceptions—Korea, Japan et cetera—but this is largely about how we get access to American data.

That means, like it or not—and many people are beginning to come to this conclusion—that the real fix for this is a cyber-evidence convention, like the cybercrime convention. That will involve diplomatic heavy lifting and an agreement, perhaps initially between America and the European Union, with other willing countries joining later as they wish, that provides a very much faster service for getting at stuff than the current mutual legal assistance treaties. For that to work, there are three things we almost certainly have to have. The first is warrants signed by judges, because that is what America expects. The second is transparency, which means that if somebody gets wiretapped you eventually tell them—when they get charged or after three years or whatever. The third is jurisdiction, because the real bugbear for companies like Google at the moment is that a family court in India gives it a warrant saying, "Please give us the Gmail of this person in Canada", who has never been to India. How do you simultaneously employ engineers in India and give privacy assurances to your users in Canada? That is why at present all this stuff gets referred to lawyers in Mountain View. That is the real problem, and it is time the Government faced up to it.

The Chairman: Professor Ryan, do you want to say something regarding an earlier point?

Professor Mark Ryan: I want to go back to the question of whether these are new powers or existing ones. Following what Dr Bernal said, one of the very huge powers that exists in the Bill is bulk equipment interference—that the state can interfere with people's computers on a bulk scale—which means that people who are not guilty of any crime, nor even suspected of any crime, may have malware put on their computers by intelligence services to collect vast amounts of data on innocent people in a kind of funnel, so that eventually criminals can be caught, but the people who are being subjected to that are not criminal at all. That seems to me to be an extremely dangerous thing in a free society. I do not think that the kind of oversight proposed in the Bill goes anywhere near being able to control that type of activity.

Professor Sir David Omand: The bulk equipment interference warrant can be sought only by the intelligence agencies in order to acquire intelligence relating to individuals outside the UK for the purpose of national security. For the sake of clarity, the Bill already restricts that.

Q83 Lord Strasburger: Sir David, your career was spent in senior positions in the Civil Service deep inside the security establishment, which probably makes you, of the panel, specially qualified to answer my question. It seems that over the past 15 years decisions were made behind closed doors to introduce several of the most intrusive and least overseen powers in this Bill without bothering to seek Parliament's approval. Why was it considered acceptable in

a democracy to bypass Parliament and introduce large-scale and highly controversial surveillance powers without Parliament's explicit approval?

Professor Sir David Omand: I can only hazard an answer, which is that the legal regime under which previous Governments operated for the past 20 years, since the 1980s, was what I would describe as legal compliance; in other words, if it could be done lawfully under existing powers that Parliament had passed, Ministers would authorise such activity, after due legal advice, regardless of party—this is not a party political matter—in the interests of national security, the prevention and detection of serious crime, and economic well-being arising from causes outside the United Kingdom. That was the regime.

It was really when the Investigatory Powers Tribunal took the case and reported that the Government's activity, in particular GCHQ, might be regarded as lawful under the individual statutes but failed the rule of law test because it was not clear, as your question implies, to the public—

Lord Strasburger: Or to Parliament.

Professor Sir David Omand: Or to Parliament. This Government have taken that to heart, and the Bill is in part the result. We have moved into a new era and I am personally very glad of that. A lot of trouble would have been saved if, say, even five years ago the codes of practice—it would not necessarily have taken new legislation—on equipment interference, investigative powers and so on had all been updated to the modern digital world. For one reason or another that was not done. The shock of discovering what was happening, for very good reason—to defend the public and our security—was all the greater. I think the lesson has been learnt.

Q84 **Victoria Atkins:** I have a question for Professor Anderson and Dr Bernal. You talked a lot about privacy and, in particular, the debate in America about privacy. One thing that strikes me about the whole discussion is that very often we are focusing, if I may say so, on the worst-case scenario as to what the intelligence services and the Government will do with people's information. What are your views in relation to the computer companies that hold all this data about us? If we google a dating agency, Google will have that information. What are your views on those bodies, because to me they are very much part of the debate about privacy?

Professor Ross Anderson: Yes. I tend to take different views of different companies because of their different internal cultures. Having worked at Google, I understand and to some extent trust the culture there.

Victoria Atkins: You worked at Google.

Professor Ross Anderson: Yes, four years ago on sabbatical, so I understand it. My colleagues have worked for other companies. Fundamentally, whether you are a company that tries to be good or a company that is a bit less scrupulous, the underlying fact is that the modern economy depends on people trusting large service companies with their data, because it is so much more efficient to have 100 million people's data in a data centre than it is for everybody to be backing up their own hard drive at home and losing their photos

and everything. That trust has to be maintained. If it is lost, the consequences could be dire for economic growth and the companies concerned.

People talk about worst-case privacy scenarios, but that is how people talk; that is how the media and politics operate—they operate by stories. The human brain is optimised for stories; it is how people remember stuff. If you get the perception out there that in the UK people who offer services have to leave a government back door, or remove the encryption if ordered, or whatever, it could be extraordinarily damaging for British business.

Victoria Atkins: Does selling people's data come into that? Are you comfortable with Google's position on that, having worked for it?

Professor Ross Anderson: Personally, I do not click on ads. If you want to go to a company that does not sell data, you can go to Apple or you can go to the trouble of having everything private. For example, I take the view that, if I am sending an email that I do not mind the FBI reading, I use Gmail; if I am sending an email that I do mind the FBI reading, I use something else. That is also the conclusion to which I think more and more users generally, and young people in particular, are coming to.

Q85 **Matt Warman:** I have a question for Dr Bernal primarily. As an example of new powers in this Bill, you said it was like following someone down the street and seeing which shops they go into. It strikes me that we have long had the power under certain circumstances for people to be placed under surveillance and followed down the street to see which shops they might go into. Could you give the Committee an example perhaps when we get back?

The Chairman: Order. There is a Division in the Commons, so we will adjourn for 10 minutes. I am sorry about that.

The Committee suspended for a Division in the House of Commons.

Matt Warman: To recap briefly, you cited the example of following a person down the digital street under authorised surveillance, which strikes me as a digital updating of analogue powers we have already. Could you offer the Committee an example that is not simply a digital updating of existing analogue powers and is genuinely novel because it is digital?

Dr Paul Bernal: It is a very important question, and there are lots of issues related to it. There are some things that we do in the real world, or the offline world, that we feel comfortable being observed doing. We have CCTV cameras in the streets, we have them in shops, and so on. We do not have them in our bedrooms, we do not have them staring at our diaries all the time and we do not have them monitoring exactly where we walk. We get the choice: do we want to go to this place where we know there is CCTV, or that place where we know there is not CCTV? That is one of the important differences.

The thing about the Internet as it is now, particularly for younger people, is that they do literally everything on it; there is no aspect of their lives that does not have an online element. If you have a system as is proposed with Internet connection records, for example, where there is some gathering of their entire browsing habit, not beyond a certain level—I hope we will get on to Internet connection records later—at least you have knowledge

about what they are doing in every aspect of their lives. When you go to the doctor, you expect confidentiality from your relationship with the doctor when you discuss your health issues. If you visit a website to research a particular health condition, that may reveal just as much about you as you would reveal to your doctor—in fact, many times more than you might reveal, because people have a sense that they can get more intimacy by doing things on the Internet than they might even be prepared to admit to a doctor.

There is another element. We talked a little about Google and others. Given the way profiling works for almost all commercial Internet companies, and the way big data analysis works, you can draw inferences from relatively small amounts of browsing data that can then be used to infer stuff that you would otherwise keep private. An example is your sexuality. You might not want to reveal your sexuality, but big data can make a probable analysis of it with a relatively small number of places you visit on the Internet.

It goes back to the question about whether we are looking at extreme cases. We are looking at extreme cases in some ways, but we are also looking at very ordinary cases. What we all do on the Internet has an impact on credit ratings, insurance premiums and things like that. They can be based on very basic information that can be gathered about how we behave.

I am sure David will say that safeguards are built into the Bill so that it can be used to do only certain things, but that is not really the whole story for two reasons. One is that data, wherever they are and in whatever form, are vulnerable in many different ways. The example that comes most readily to mind, because it is so recent, is TalkTalk having been hacked, and holding exactly the kinds of records that we are talking about. That information is ideal for ID theft, credit card fraud, scamming and things like that.

If we gather those Internet connection records, we are basically creating a very targeted database, which says on the front, "Hack me, please, if you want to get ideal information for these kinds of crimes". We need to be careful not just about what we think the Government are going to do. Like David, I trust to a great extent our security services and police, but we are creating something that can be misused by other people, not just by them. There are many ways in which that can happen.

Q86 Suella Fernandes: In terms of legality, the issuing of warrants is subject to the test of it being necessary and proportionate. In light of that, what is your view on its compatibility with proportionality as required under the ECHR?

Professor Sir David Omand: Proportionality and necessity are in the Bill. They are written in, as they are in the current legislation. Dr Bernal's examples were very good ones of why digital mass surveillance is a thoroughly bad idea. Thankfully, it does not happen now, and under the provisions of this Bill it could not happen in the future either. The question that I suggest the Committee really needs to address is how proportionality is assessed—precisely your question—not just in relation to the granting of a warrant but the whole process through which the selection of material for examination by human beings—the analysts—takes place. The IPT, the independent court, has examined this; senior judges who oversee interception have examined it, and they are satisfied that the current procedures are consistent with the Human Rights Act, Article 8 and thus respect privacy. Equally, there is no reason why the provisions cannot be applied in practice in ways that remain consistent.

The decision on proportionality and necessity rests with the person signing the warrant. The Home Secretary has made her view clear in the Bill. I am disappointed that she decided that she had to sign police warrants and that they would not go direct just to the senior judge for approval, which was our recommendation in the independent review commissioned by the former Deputy Prime Minister, and that would be more consistent with David Anderson's review. I strongly believe that the Home Secretary or the Foreign Secretary, as appropriate, should sign the warrants relating to national security and the work of the national intelligence agencies, for which they are statutorily responsible to this House. The police service is in a different constitutional position, and I would have thought that purely police matters could go straight to the judge. It is no harm that the Home Secretary signs as well; it is just additional work.

Dr Paul Bernal: Can I go back to the question of proportionality? One of the key things is not just about the warrant to access the information. One of the key elements of proportionality is the gathering and holding of the information itself. The CJEU has consistently—even more so recently—held that the holding and gathering of the data engages Article 8, and that indiscriminate generalised holding and gathering of data is contrary to fundamental rights. That was held in Digital Rights Ireland; in the Schrems case it was part of the key reason why the safe harbour decision was invalidated. This is not because they have some perverse view that does not match with reality but that the European Court has started to understand the impact of holding all this personal data. It is not just the warrants—to a degree, I agree with David about the warranting process; it is the gathering of the data that I disagree with, particularly the way Internet connection records are set out. All this data seems to me to be gathered on the assumption that that is all okay and it is just the accessing we need to deal with. I cannot see how this law would survive a challenge in the CJEU on that basis.

Professor Sir David Omand: I very strongly disagree. I am not a lawyer, but it seems very clear to me that the Schrems and the Digital Rights Ireland judgments do not bear on the point that has just been made. Those judgments did not consider the question of proportionality of collection and selection, which is not indiscriminate collection of data willy-nilly. You might want to take advice on that.

Professor Mark Ryan: I want to comment on the bulk provisions of the Bill, because they allow for the collection and automatic processing of data about people who are not suspected of any crime. Therefore, I do not think it is correct to say that this is not a recipe for mass surveillance. It is the processing of data about everybody, and in my opinion that is mass surveillance.

Professor Sir David Omand: But it is not processing data about everybody.

Q87 **Baroness Browning:** We have covered quite a bit of my question about definitions. Clearly, we have differing views on the panel. Sir David, in your evidence to the Science and Technology Committee I believe you suggested that somehow you would never get a perfect definition, and in the absence of that a pragmatic approach should be taken. Do you want to identify the balance between being safe and being practical?

Professor Sir David Omand: The starting point has to be the value of communication data both to the police and to the intelligence agencies. The police evidence is very clear. It has

huge importance in ordinary crime as well as in countering terrorism and cybercrime. From that starting point, we have to have an authorisation process that can cope with the number of requests, which is over 500,000 a year, so talking about requiring warrants to be signed by Secretaries of State or senior judges is not appropriate. The justification for that was that it is less intrusive to look at communication data than to look at content, and that principle is reflected in the Bill.

The point I was making to the Science and Technology Committee is that there will be some hard cases, and Professor Anderson gave some examples of precisely that. If you move the cursor too far over to be so restrictive, you create a real problem about the authorisation of data communication requests. If you move it too far the other way, you get the equal and opposite problem of not sufficient authority being applied. The cursor is more or less in the right position, because it has taken the RIPA 2000 definition of who called whom, where and what, and transferred it to the computerised age of which device contacted which server up to the first slash of the address, but there will be hard cases. I was suggesting to the Committee that you have to be pragmatic and ask whether the overall public interest in the authorities and police having this information, which is vital for upholding the law and bringing people to justice, balances the fact that you may occasionally have a hard case. In my view it certainly does.

Baroness Browning: If we get the definition right and if we get the clarity that the panel seems to feel is lacking at the moment, do you think that will serve us for now, or will we have to keep revisiting this?

Professor Sir David Omand: For the sake of clarity, I think the definitions are clear; it is reality that is fuzzy. The parliamentary draftsman has done a very good job trying to clarify this. I am not sure you can make it any clearer.

Baroness Browning: That is very clear. Thank you.

Dr Paul Bernal: This is a really important element. Sir David said that communications data was less intrusive than content. I do not think that is true. They are differently intrusive. There are several reasons communications data can be more intrusive. One is that it is by its very nature more suitable for analysis and aggregation. You can do more processes to it than you can to content. That means that it is subjected to what we loosely called big data analysis. It is also less hard to disguise in some ways. You can talk about a coded, not encrypted, message to somebody. In England we do this all the time; when we say “quite”, it could mean a million different things depending on the context. You cannot do that so easily with communications data. That means that sometimes you can get more information out of communications data than you can from content. I do not think you should be under any illusions that somehow it is okay to have as much communications data gathered as possible but not okay to get content. They are different things. For individuals, sometimes content matters more; en masse, communications data matters more.

The Chairman: Before you came in we were discussing the differences between communications data and content, but the drafters of the Bill and the Government who sponsored it seemed to indicate that there is a significant difference in terms of people’s

privacy with regard to what is written by them and to them, as opposed to the hows, the wheres and the whens, but you are contesting that.

Dr Paul Bernal: I am contesting that. I would say that it can be worse. You have at least some control over what you write, whereas for communications data largely you have very little control over it at all. It is a different sort of intrusion.

Q88 **Baroness Browning:** From the point of view of the speed at which things change, could you indicate whether you think that even if we had an imperfect definition, in your terms, we are going to have to keep coming back to legislation more quickly to update it? Is that a danger?

Dr Paul Bernal: Frankly, yes.

Baroness Browning: Do you think we will keep coming back to this?

Dr Paul Bernal: I think you will be coming back to this and you should be, because things change in so many different ways. This is not the sort of law that you can set down and say it will last for 15 or 20 years without amendment, because the technology is moving too fast; people's behaviour is changing too fast.

Baroness Browning: May I bring you back to Sir David's point? Seeking perfection is perhaps something that we should compromise with pragmatism.

Dr Paul Bernal: You should, but you should compromise it by adding extra oversight rather than by accepting a loose definition, by making sure you can monitor what the intelligence and security services and the police are doing so that pattern of behaviour matches the intent behind the law as well as the definition. This is part of Lord Strasburger's analysis of how powers have grown without parliamentary approval. It is very easy and we have seen it historically again and again. People have not been watching what is going on and you need to continue to monitor things. I am not yet convinced that the oversight arrangements here are strong enough to do that. The idea of, if not a sunset clause, a revisiting clause of some kind might be worthwhile, and also monitoring the monitors: how are the oversight arrangements working?

Q89 **Stuart C McDonald:** Turning to communication service providers and the requirement that could be placed on them to store up to 12 months' worth of communications data and Internet connection records, how feasible is it for providers to do that?

Professor Ross Anderson: It could be extraordinarily difficult and expensive if they are to do what they are advertised to do. We are told that Internet connection records will enable the agencies and police to get past what is called carrier-grade NAT, which is a technique whereby the IP address of your mobile phone might be shared with 1,000 other mobile phones, the idea being that, if someone does a bad thing online on Monday, you ask O2 and they say that it could be any one of 1,000 phone numbers, and, if the person does another bad thing on Wednesday, you have another list of 1,000 phone numbers and you say, "Aha! The common number on the two lists is this one". It is not going to work that well, first because you will find hundreds of common numbers on the list; and, secondly, if you want to relate that to things people have done on other service providers, you have to

relate it to an ID on Google, a handle on Twitter or a logon for Facebook. For that, you would have to require the communication service providers to store very much more data than they do at present. You would have to get them to store precise time stamps, addresses and so forth, which they will not do.

ICRs will not work as advertised. What they will do is create an extraordinary capability power for investigators to say, "Show us all the websites that these two bad people have visited in the past month and all the other people who have visited the same websites". If you want that capability, which appears to be what is intended, you end up requiring lots of people to store lots of stuff. There is, first, the issue of cost if you are to remunerate communication service providers in Britain; and, secondly, there is the likelihood that service providers overseas will refuse outright because it would be too much effort and energy to redevelop their systems, and Britain is only 4% of the market anyway.

Dr Paul Bernal: The Danes are the people who have got closest to doing this, and I would recommend, if you can, to get one of the witnesses from the Danish abandoned attempt. They ran it for nearly seven years and got almost no useful information out of it, but there was a huge cost, even though they were warned beforehand by the ISPs, as I believe they will be here, that this is not a practical proposition and is not likely to be an effective one.

Professor Sir David Omand: The Committee will discover, if they do that research—I hope they will—that the model the Danes chose is not the model I strongly suspect the Home Office would choose. The Danes themselves are revisiting it at this very minute because they may find post-Paris that it is necessary to go back and look at it.

Q90 **Matt Warman:** I want to talk a little about encryption or decryption. Do you think it is reasonable for Government even to ask communications providers to provide unencrypted material for something that is currently encrypted?

Professor Ross Anderson: There is a power in Section 3 of the RIP Act which allows them to do that. As I remarked earlier, Parliament saw fit to hedge it with very stringent safeguards. Nowadays, it would be much more difficult, because many service providers encrypt stuff by default. They do so not out of any particular malice towards agencies but simply to stop other people stealing their ads and customers. It has just become the commercial default; it is what everybody expects. With messaging services, everybody increasingly expects stuff to be encrypted end to end. The Government of Kazakhstan have recently decreed that everybody has to install the Kazakhstan Government's cert on their machine from 1 January. I predict that if you have an iPhone in Kazakhstan you will suddenly find that none of the services works. That will be worth watching.

Matt Warman: Sir David, do you have any thoughts on whether we are likely to get anything meaningful out of demanding unencrypted data from people who currently encrypt it anyway?

Professor Sir David Omand: Of course, you will be distinguishing between content data and communications data, which clearly has to be delivered in a form in which the authorities can use it. If we are looking at content data, as far as I can see there is no back-door encryption provision in the Bill. The Government have said that they are not seeking it. I know the agencies are not seeking it, so as end-to-end encryption spreads it will get harder

and harder for the authorities to be able to access unencrypted content, even for their highest priority suspects. That is a fact of life.

Does that mean that the authorities should have no power to seek such information, and to do their best in cases where it might be available? That is the approach I would commend to the Committee. It is a power to seek, but I do not think it is in Parliament's power to insist that all encryption can be bypassed, nor would it be a very sensible thing to ask for in terms of the national economy and the need for the Internet to be secure. There will be specific cases where it will make sense and information could be made available, and the Bill should provide for that.

Matt Warman: To be clear, in general you do not see the Bill as providing the back door that people have spoken about.

Professor Sir David Omand: No, I do not.

Dr Paul Bernal: Many of the companies concerned do not share Sir David's view, and that is one of the reasons why some of them are distinctly disturbed by news of the Bill. One other thing that we need to be very clear about—Professor Anderson has already referred to it—is that we do not want to put British companies at a disadvantage, because they are more likely to be subject to the force of British law than a company in California or Korea. If we put the power in place to allow them to do it, they are disadvantaged, and that is not good for anybody.

Matt Warman: Which only emphasises the need for clarity, does it not?

Dr Paul Bernal: Clarity is what is needed.

Q91 **Matt Warman:** To move on to equipment interference, what does the panel understand that to be?

Professor Ross Anderson: It is basically hacking or the installation of malware, or what the NSA calls implants and what we call remote administration tools in a machine. If I am a bad person, the police would be able to say to O2, "Put an update on the android on Professor Anderson's phone", and that would enable them remotely to turn it on, use it as a microphone or room bug, or look at me through the camera, collect my location history and all the rest of it. What is more, as we get digital stuff in more and more devices they could do the same to my granddaughter's Barbie doll; they could do the same to your car or your electricity meter. It is open season on the Internet of things. It goes without saying that the controls around that need to be very carefully drawn; otherwise, it undermines trust. If UK producers of stuff can have their arms twisted to provide a capability to put implants into stuff, why should people buy stuff from Britain?

Professor Sir David Omand: I agree with the point Professor Anderson makes about the need for careful oversight of this, but the power already exists; it is already in use under existing statutes, including the 1994 Act. It is of inestimable value to the intelligence agencies, particularly on national security addressed to targets overseas where there are

legitimate demands for intelligence. Some 20% of GCHQ's output benefits from that kind of technique. There is nothing very new about it.

Dr Paul Bernal: There is nothing new about it, but there is something new about our behaviour and the technology we all use. Twenty years ago I was not using anything that was encrypted at all; now half the stuff I have on my phone is encrypted by default, and another batch is encrypted by choice by me, so for normal people this now becomes relevant when it was not relevant before.

Professor Ross Anderson: What is new is that we found out about it thanks to Edward Snowden, and GCHQ admitted that it was doing it just in the last month or two, thanks to the case currently before the Investigatory Powers Tribunal. People are beginning to get worried about it, and with due cause.

Q92 **Lord Strasburger:** Gentlemen, can you help me out with bulk personal datasets? The Bill and the Explanatory Notes are very vague about that. The ISC report was rather vague about it—it was hugely redacted. The Home Office will not tell the Committee the identity of the databases it is scooping up, so it is very difficult for this Committee to assess the proportionality, risks and intrusiveness of the collection of bulk personal datasets. Does anybody know what they contain? Do they contain medical records? Do they contain bank records? What do they contain?

Professor Ross Anderson: For starters, we know that the police have access to things like credit reference and DVLA records. That is public knowledge. Secondly, they have access to medical stuff. They have had that since 1996. At the time, I happened to be advising the BMA on safety and privacy and that sort of thing came through. Thirdly, in any case, hospital medical records were sold on a wide scale in the care.data scandal last year, and it would have been rather negligent if GCHQ had not grabbed a copy on its way past. Fourthly, it is well known that some kinds of bank records, in particular all international financial transactions, are harvested on their way through the SWIFT system.

Professor Sir David Omand: Not true.

Professor Ross Anderson: This has been a matter of enormous contention in the EU and elsewhere. It is only to be expected. If I were, for example, an investigator for the FCA, I would want everybody's bank statements too.

Professor Sir David Omand: Chairman, it is important not to allow fantasy to intrude at this point. The central bank governors responsible for the SWIFT system agreed that that system could be searched for specific transactions of known criminals and terrorists. That is public knowledge. All SWIFT data is not scooped up.

Lord Strasburger: Perhaps we could impress on the Home Office the need for the identity of these databases to be revealed.

The Chairman: That is something that we would have to do in private session, but I take the point that there is a serious difference of view between the witnesses on what is a hugely important subject.

Q93 **Dr Andrew Murrison:** I am going to be fairly brief, because I think we have covered quite a lot of this already. I refer to the international dimension. We sit here thinking we can make various laws and regulations, but we are talking about a global industry. Referring to some of your previous comments, could you reiterate the likely reaction of the international community to the Bill, in particular the feasibility of gathering ICRs, given that it is entirely in the gift of companies whose headquarters are not in the UK?

Professor Sir David Omand: We took evidence on this as part of the independent surveillance and privacy review run by RUSI and we got a variety of answers from international and British companies. Some of the companies said that as a matter of corporate social responsibility they wanted to be in a position to provide this kind of information for the purpose of preventing serious crime and terrorism, but they felt extremely nervous about doing it without a firm legal basis on which warrants or authorisations would be made. Other companies said that as a matter of company policy they did not believe their data should be made available to any state or law enforcement authority. You have a variety of views. The provisions of the Bill, which include the provision that the Home Secretary can make judgments about what it is reasonable to expect, will be partially successful; but they will not be completely successful, because some companies will simply refuse, and I cannot see the British Government attempting to launch civil actions against major players.

Dr Andrew Murrison: Presumably that means that the disinclined would note those who were complying and those who were not and go for those who were not.

Professor Sir David Omand: The intention is not to make public the companies that comply and those that do not.

Professor Ross Anderson: We all know the companies that will comply. They are the ones that get large amounts of their revenue from Governments, or that rely on Governments for capture regulators—companies such as IBM, BT and those set up several generations ago. Companies that have been set up in the past 20 years think differently because they have a different culture—the Silicon Valley culture. Their money comes either from their users directly or from advertising—from their users buying stuff or being advertised to—and they take a completely different view. It is not much good getting BT on board if all BT is doing is providing a piece of copper wire from people's houses to where the real action starts, so it is the view of the big American service companies that matters more than most. They are going to drag their heels.

There is the issue of foreign Governments. There is also the issue of what happens to small start-ups in the UK, which is absolutely crucial. For example, about five years ago one of my postdocs set up a security start-up. Because of the arm-twisting that the agencies have always indulged in, he decided to set up a coding shop in Brno in the Czech Republic. More and more people will be doing that, simply as a matter of default. You cannot run a tech start-up nowadays unless you have a marketing operation in North America, because that is where you make your first sale and most of your initial sales. If we create a regulatory regime where it is only common sense for people to put their coding shop, their

engineering, in North America, Seoul, Mumbai or wherever, the cost to us directly or indirectly down the stream of time will be huge.

Dr Paul Bernal: We have to be aware of where things are moving. There may be a number that are co-operating willingly now, but that will shrink. More and more companies are likely to say, "No, we are not going to give this", and they will be the bigger and more successful ones. You make yourself a hostage to fortune by assuming that this will end up functioning.

The Chairman: Thank you very much indeed. I thought the whole session was absolutely riveting. You have given us an enormous amount to think about. Obviously, you have very different and varying views on the issues before us, but you highlighted issues that very much need highlighting. I know that members of the Committee are grateful to all four of you for giving us your very robust and significant views on this important Bill. If you would like to add any written evidence to supplement what you have said, we would be more than happy—indeed delighted—to receive it. Thank you very much indeed.

Matthew Ryder QC (QQ 186-196)

Evidence heard in public Questions 186-196

Oral Evidence

Taken before the Joint Committee

on Wednesday 16 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Lord Butler of Brockwell, Bishop of Chester, Lord Strasburger.

Witness: **Matthew Ryder QC**, gave evidence.

Q186 **The Chairman:** A very good evening to you. I am sorry that we are a little later than we thought, but we have had a couple of fascinating sessions. I have not the slightest doubt that this will be equally fascinating. You are all most welcome to the Committee. As you know, in these situations different Members of the Committee will ask different questions, but I am going to ask a very general one, which perhaps gives you an opportunity to make a general comment on the Bill that the Committee is considering, if you wish to. Aside from the new powers on the retention of internet connection records, in your view, does the draft Bill consolidate existing powers or extend them? In answering me, if you wish to make any more general comments, please do so.

Matthew Ryder: The answer to that question depends slightly on, when you talk about extending the powers, whether you mean extending what the security services and the authorities are already doing and what they say is authorised, or what others would say is currently authorised under the existing legislation. There is a dispute and lots of litigation about what is or is not currently authorised under the existing legislation.

My view would be that there are a large number of new powers that are not properly authorised within existing legislation. Just to go through them with headlines, in Part 1 of the Bill, thematic warrants are allowed in relation to Clause 13. There is not a thematic warrant provision for targeted surveillance and targeted interception within RIPA. I know that the Government say that, if you cross-reference Section 8(1) with Section 81, you can find group surveillance as part of targeting but, realistically, thematic warrants are something new, and the idea that you could target people as groups by their activity is something new in part 1 of the Bill. It is important because, conceptually, it is anathema to the existing culture of surveillance that has been going since the 18th century in this country. If we are to move in that direction, it needs an informed parliamentary debate about it, to decide if we want to go in that direction.

Secondly, mass surveillance or bulk interception—whatever you want to call it—under Part 2 of the Bill is essentially something new. I understand—I was involved in the case and litigated the case in the IPT last year—that the Government say that bulk interception or

bulk collection is permitted under Section 8(4), but there is a dispute about that. There is a case on its way to Strasbourg. It has been communicated in Strasbourg. There are many of us who would say that it was not set out very clearly, if it was permitted at all, in RIPA.

Part 5, on equipment interference, is really new. It has really emerged only since the draft code of practice was published in February 2015 in response to ongoing litigation. It turns out that the Government's position on the existing power is that it is a very broad power, under Section 5 of the Intelligence Services Act, combined with the draft code that they published on the door of the court in February 2015, so equipment interference is new. It is a very significant power that requires a lot of scrutiny and debate.

Part 7, on bulk data sets, is essentially new, has not been regulated before and is not in the existing legislation in any meaningful way. The power to have access to bulk data sets and how they would be defined is something new.

I missed Chapter 2 of Part 6 on bulk communications data acquisition. That is essentially new. In other words, the large collection of communications data in bulk is something that was not clear from any legislation before. That is essentially being regulated for the first time, under this Bill.

Finally, it is arguable—this is more debateable—that Clause 189, which is the clause that has tech companies particularly concerned, is if not new then certainly of new significance, because it requires telecommunications service providers to maintain their capabilities and combines that maintenance requirement that existed in RIPA with a new definition of a telecommunications service and those who are providing that service. It is broadened out by Clause 193(12) to those who are allowing those communications. That means that those companies that simply have communications apps that facilitate communications through the internet, such as Facebook, Apple or those sorts of companies, may be caught in a way of maintaining their capability that they had not imagined before. That opens up the question of whether encryption is engaged in relation to that issue and, if it is not in the Bill as it stands, in due course whether that is a concern. In summary, there is quite a lot here that is very new and these powers are important. They are significant and, therefore, because they are new, they would require debate.

Martin Chamberlain: That was a very comprehensive answer that enables me to be much briefer. The answer to whether and to what extent the Bill contains new powers is very difficult, for this reason. In the run-up to the tabling of the Bill a number of things that nobody knew the agencies were doing, they were revealed to be doing under the existing powers. There has not been time for some of the things that we have very recently found out the agencies are doing to be tested in legal proceedings. I am thinking there particularly about the use of the extended definition in Section 80 of RIPA effectively to enable thematic warrants to be issued, and the use of Section 94 of the Telecommunications Act 1984, which is something we found out about for the first time in the immediate run-up to the tabling of this Bill. As to whether those activities that we now know have been undertaken by the agencies are lawful under RIPA, the answer is that it has not been tested and so it is very difficult to know.

Generally speaking, whether the Bill confers new powers is, with respect, not a terribly helpful question. One of the important purposes of this Bill is to get a democratic mandate

for things that have not yet had a democratic mandate. Whatever you might say is the correct judicial interpretation of some of the old powers, certainly it can be said, without any doubt, that quite a lot of the things in this Bill are things that nobody in these Houses of Parliament has examined the justification for, to date. Are they new powers? One can debate that. The courts have not had the opportunity to debate it, in many instances. They certainly are new in the sense that they have not had a democratic mandate, in many cases.

Peter Carter: Needless to say, I agree with all that has been said, so I shall be even shorter, I think. This Bill is important, because it enables the democratic process to take control of what has hitherto, to a large extent, been a hidden exercise of what is known as a prerogative. It is about time that the prerogative powers were brought to heel and this is a good way of doing it.

Insofar as this Bill brings within the ambit of the law practices that hitherto have either been questionable or possibly outside the law, there is a huge amount to commend it. Only if the kind of activities that this Bill encompasses are subject to law and lawful control, and therefore lawful monitoring, can it be said that these powers are being exercised in a truly democratic way. We need the powers in this Bill, to some extent or another, to combat serious crime, terrorism and actions against the state. The exact extent is a matter for political debate, as well as legal debate.

One of the problems and one of the ways in which the current drafting of the Bill, potentially and exponentially, will extend the powers is in the definitions clause, Clause 195, which includes a definition of data. As Matthew has said, one of the things that appears to be an extended power is the bulk acquisition of data. Data is defined in Clause 195 as including any information that is not data. Therein lies a problem.

Graham Smith: I am going to be slightly longer. I have identified quite a few new aspects that are potentially new powers in this. First, although the question caveats out internet connection records, we do need to understand that, when one looks at Clause 71, which is the power to issue data retention notices, and one compares it with the existing data retention powers in DRIPA, as amended by the Counter-Terrorism and Security Act of 2015, and if one adds internet connection records to that, Clause 71 still goes far beyond adding internet connection records to the existing data retention powers.

Although this has been presented as something to enable the retention of internet connection records, it goes far beyond that in five or six different ways. Perhaps most significantly, the existing DRIPA powers are restricted to a few types of human-to-human communication—internet email, internet access and internet telephony. This would catch all the background activities on my smartphone that happen when it is sitting by my bedside when I am asleep, when I am away from it, whether it is receiving notifications, getting software updates or anything of that sort. It would capture and cover any machine-to-machine communication, which if you look forward to the internet of things would cover my connected home thermostat or my car checking if it needs a software update. Essentially, anything connected to the internet or indeed any other type of network would fall within Clause 71. It now applies to private services and systems, as well as public, and of course the power to require data to be generated for retention, not just retained, is completely new. The previous limitation to retaining data generated or processed within

the UK has been removed, so Clause 71 is very much broader than one might think by just referring to internet connection records.

Other new and extended powers are technical capability notices, under Clause 189. At the moment, under RIPA Section 12, capability notices can be given to support interception warrants and nothing else. Section 189 will apply also to all the new types of thematic, targeted and bulk warrants, under Parts 5 and 6, and will also apply to support the acquisition of communications data under Part 3. All of that is new.

In bulk interception, there is a new power. I call it a new power, but it comes as a result of the warrantry definitions; however, there is effectively a new power to extract related communications data from content and to treat it as related communications data. For instance, if I send you an email saying, "Here is somebody's email address", that is part of the content of my email, but the email address can be extracted from the content and then treated as related communications data. That is very significant, because most of the restrictions on examination of content do not apply to related communications data, so it is very significant. That is replicated as well in the new bulk acquisition and equipment interference powers, which talk about equipment data, which is more or less equivalent to related communications data. There is the power to extract equipment data from the content that is acquired in that way.

Lastly, there is the extension generally through the knock-on effects of the expansion of the definition of telecommunications operators in the draft Bill.

The Chairman: Thank you so much. They were some very useful answers.

Q187 Matt Warman: Given that we cannot agree on what is meant by new, I slightly hesitate to ask this. The Committee has been blessed with lots of different interpretations of what judicial review will mean in the context of this Bill. What do you think judicial review terms would mean, as far as the authorisation of warrants would go, in this new Bill?

Martin Chamberlain: You have just heard from David Davis about Lord Pannick's article in the *Times*, where he suggested that, in this kind of context, the judges would be applying a high intensity of review. One can explain it in this way: whenever a judge is applying a judicial review standard, there is a spectrum of different types of intensity of review. At one end of the spectrum, there is very light-touch review, which David Davis accurately described as, "Don't touch it unless it's totally barmy". Then at the other end of the spectrum, there is a real rolling up of the sleeves, getting into the detailed kind of review, where the judge comes close to substituting his or her own judgment for that of the ministerial decision-maker.

Practically any judicial review practitioner will tell you that, in practically any judicial review case, a key point of contention between the parties is where on the spectrum that case lies. Is it a light-touch case, is it an intensive-review case or is it somewhere in between? David Pannick's article in the *Times* suggests that this would be an intensive review kind of case. David Pannick is generally right about most things, but I would venture to suggest that you need to apply a bit of caution to whether that is correct in this context. Certainly it is true that a warrant authorising interception involves an invasion of someone's privacy,

but it does not involve the kind of restriction of liberty that you see in, for example, a control order case or a TPIM.

The Committee suspended for a Division in the House.

Matt Warman: You were in full flow on what judicial review is likely to look like in this context.

Martin Chamberlain: I have explained that there is a spectrum in judicial review, in terms of intensity of review, with very light-touch review at one end and high-intensity review at the other. David Pannick thinks that, because of the privacy context, we would be in the high-intensity part of the spectrum. I question really whether that is correct. The reason I question it is this: the matters under review, under Clause 19, are whether the warrant is necessary and whether the conduct authorised is proportionate. If you just concentrate on that second question, you are asking yourself the question as a judge reviewing this warrant whether the national security benefit to be derived from the warrant is proportionate to the intrusion into privacy that it involves. That is, to my mind, typically the kind of question on which judges will give a great deal of what used to be called deference—some of the later judgments deprecate that term, but leeway or latitude, however you want to put it—to the elected Minister. That is what would normally happen in judicial review. There is a House of Lords case called *Rahman* that makes that point. Where you are looking at proportionality assessments by a Minister who is accountable to Parliament, you apply a very light-touch review.

The touchstone, if you really wanted to get an interesting answer to this question of where on the spectrum it lies, is to ask someone from the Government what they think and see if they would be willing to give the kind of parliamentary statement that could be relied on in subsequent legal proceedings, to say that what they meant by judicial review was intensive review. I doubt whether you would get them to say that, because I suspect they would want to reserve the position to argue in front of the commissioners that it was a light-touch review that was intended.

Peter Carter: I hope Lord Pannick is correct, but I also fear that it is so uncertain that he may not be. This is not an area in which uncertainty can possibly be allowed to be sustained. One of the problems about judicial review is a problem that was created by Lord Judge last year because, in a decision called *Regina v L*, a decision in the Court of the Appeal in which he gave the judgment, L was somebody who as a young woman who had been trafficked for exploitation. The question was whether it was right that she should be prosecuted for an offence that she committed as a result of her exploitation, which we would now call modern slavery. The issue was what test is to be applied to the decision of the Crown Prosecution Service to proceed with her prosecution, even though all the circumstances demonstrated that she was a victim of exploitation. The test to be applied is one of judicial review.

There was the kind of discussion that we have heard about: on the one side this; on the one side that. Lord Judge said that we are going to apply in this case a test that is not the conventional judicial review; it is something different from that. The difficulty was that he did not say what it was. I do not know anybody at the Bar, who practises in that area of

law, who understands what the test with which we are left in that area of law is. What I suggest is that the simplest way of removing this ambiguity is to suggest an amendment that you simply delete the words about judicial review.

May I go back to the stage about how the judicial commissioners will consider this? It starts off with reviewing what? A decision by the Secretary of State. Normal judicial review is a review of a decision and the reasons for that decision. Are those reasons irrational or are they rational? Do they include considerations that are immaterial or are they centred on considerations that are central to the issue in point? I do not think there is any provision in this Bill for the Secretary of State to give reasons for his or her decision. The judicial commissioner will not be reviewing reasoned decision. The judicial commissioner will be reviewing the decision and, therefore, ought to be reconsidering from scratch whether or not it is appropriate to authorise this warrant and doing so by applying the test of necessity and proportionality.

There is one slight twist about this because, by Clause 169(5) of the Bill, "In exercising functions under this Act, a Judicial Commissioner must not act in a way which is contrary to the public interest or prejudicial to … (a) national security, (b) the prevention or detection of serious crime, or (c) the economic well-being of the United Kingdom". I cannot imagine for a moment that any judge or judicial commissioner would act in a way that is contrary to the public interest, but who is to determine and who is to assist the judicial commissioner on what is national security, what is in the economic wellbeing of the United Kingdom, particularly if the judicial commissioner is not assisted by reasoning from the Secretary of State? If there is to be reasoning from the Secretary of State, how long is this process to take and why not simply remove the Secretary of State from the process?

Matthew Ryder: May I just make two very short points on this? The first one is that the role of the judge in judicial review, when it has been explained, might be slightly confusing in the sense that there is talk about deference. The question might be what the judge would add in making a decision, if he is going to be so deferential. That is to do with the role the judge has in judicial review, versus the role that the judge would have if the judge was having to authorise it themselves.

I have drawn an analogy here, because it goes back to some of the discussion we overheard from the previous session. There are times when this conversation seems as though it is discussing the difference between political accountability and judicial accountability. One has to remember that the authorisation, in this process, is one very small part of an overall operation, the vast bulk of which is not decided by the Home Secretary or a politician, but is decided by police and judges.

For example, Schedule 5 to the Terrorism Act which is the part that controls terrorist investigations, contains a large number of provisions, production orders and search warrants, including producing material from journalists, all of which are decided by a judge. Those can be much more intrusive, in some circumstances, and much more serious than intercepts, but we trust that to the judge. In serious crime operations, we trust search warrants and production orders to a judge, for a judge to make that decision. The judge does that not by deference to a ministerial decision but by having their own role in terms of making that decision for themselves, and it is a system that works very well with serious crime and under Schedule 5 of the Terrorism Act. That is why one can be led down a

cul-de-sac in thinking that we are choosing here between a brand new type of judicial authorisation or judicial role, when previously it had always been the Home Secretary. In reality in terrorist investigations and in serious crime, it is judges and police who are having to make those decisions and who are accountable for those decisions—sometimes life and death decisions.

Q188 Victoria Atkins: I should declare that Peter Carter and I were in chambers together. Mr Carter, you have talked about there not being any provision in the Bill that you can identify for the Secretary of State to give reasons. I have to say, listening to that, I thought, "Crikey, this is a lawyer's paradise". Is it not? We heard from Mr Davis earlier. He estimated that there are 2,300 intercept warrants a year that the Home Secretary does, which equates to nine a day, in addition to all their other duties. If the Home Secretary is having to sit down and write out reasons, in the way that you and I understand as lawyers, I fear that would be a real burden, adding bureaucracy in what is a highly dynamic environment. Is it not better to look at the evidence from the security services or whoever is making the application? Look at that and then the judge looks at it again—the same evidence—and makes their decision according to the evidence placed in front of them by the security services.

Peter Carter: I entirely agree. We do not want this to be a lawyers' paradise. It is going to defeat, not assist, the end. If the law is clear, there is less room for lawyers to get involved. You do not want lawyers getting involved to try to disentangle what ought to be a clear and transparent process for those who need to know about it. My only slight difference of opinion with what you suggested is I do wonder whether the Secretary of State needs to be involved at all, other than in those things that involve the security services.

Q189 Suella Fernandes: I have a question; I think Peter and Martin dealt with judicial review. We have heard evidence from Lord Judge and Sir Stanley Burnton, who have stated that they think it does strike the right balance, but proportionality involves a balancing exercise—a consideration of the objective and whether the objective is sufficiently important to justify the intrusion, whether the measures are directly related to the objective and ensuring that it goes no further than what is necessary. Do you not think that that encompasses a very clear and balanced assessment of the decision to issue a warrant?

Peter Carter: I do and those words are perfect, provided they are left alone.

Martin Chamberlain: I have to say that I am not quite so sanguine that the word "proportionality" necessarily connotes a high-intensity review. Within the case law on proportionality, under the Human Rights Act for example, there is still a very broad spectrum of intensity of review and, sometimes, even though the court is looking at proportionality, it gives the decision-maker considerable latitude. In other contexts, it gives the decision-maker rather less latitude.

The problem with simply saying that the standard to be applied is judicial review is that we do not know what arguments the Government will make to the judicial commissioners, and it is quite possible that the Government will say that this is the context, balancing the needs of national security against the intrusion into privacy, where you have to accord considerable latitude and discretion to the elected Minister, and where the judge really should not interfere, unless the Minister has obviously struck the wrong balance.

Suella Fernandes: Just by way of follow-up, would you confirm for the record that, in the process of judicial review, a judge would have access to the same information that was before the Minister throughout the original decision-making process? Is that your understanding of judicial review?

Peter Carter: Victoria Atkins made the point that this is a dynamic process and I entirely agree it is. Given the reality of the situation, particularly if it is a security service application for a warrant, it may well be that, by the time it gets to the reviewing judicial commissioner, which may be 15 minutes or half an hour after the Secretary of State has made a decision, further information is available. The judicial commissioner must take account of all the information that is then available, just in case there has been a shift—either augmented information or something that turns out to need correcting.

Q190 Lord Butler of Brockwell: When Mr Carter read out Section 169(5), saying, "In exercising functions under this Act, a Judicial Commissioner must not act in a way which is contrary to the public interest or prejudicial to—(a) national security, (b) the prevention or detection of serious crime, or (c) the economic well-being of the United Kingdom", I thought to myself, "Crumbs, that really is going to shackle the judge". It is certainly putting pressure on him to approve the warrant, but then I looked down and Section 7 says that that subsection does not apply "in relation to the functions of a Judicial Commissioner of—(a) deciding whether to approve the issue, modification or renewal of a warrant or authorisation". Perhaps you did not intend to mean that it was going to shackle the commissioner.

Peter Carter: No, I do not think it is. What I was concerned about was any suggestion, as perhaps had been made by one of the previous witnesses, that judges were going to be bowled over by a suggestion that this is for national security and, therefore, you must not intervene. The point is that the fact it is there will not prevent the judges from having a rigorous and robust appraisal of the information that is before them, before they make an authorisation or not.

Lord Butler of Brockwell: You are saying that this does not shackle the judge. It will enable the judge to reach full discretion.

Peter Carter: I think so. I hope that the reference to "contrary to the public interest", in any circumstances, would not be something that a judge would find difficult to understand.

Matthew Ryder: I was just going to say, in relation to the point you are making and the point made by Ms Fernandes, it is important to bear in mind that a judge in this position may have access to material, but a judge is not making his own assessment of the facts in judicial review. In the situation where a judge is assessing a search warrant or a production order in relation to something very sensitive, like Schedule 1 to PACE, which could be obtaining material from a journalist, or Schedule 5 to the Terrorism Act, which could be very sensitive and very serious, a judge has the evidence but then assesses that evidence. If the judge thinks the evidence is not sufficient, he could call for more or could look at it.

In a judicial review situation, the judge is essentially bound by decisions and assessments of facts that have been made by the Secretary of State and is applying judicial review principles—which, as Martin rightly says, can be on a range of scrutiny—to that assessment that has already been made of the facts.

The final point to bear in mind is that, normally in judicial review, there is an element of an adversarial process. In other words, the judge is assessing it with somebody making representations in relation to the other side. There will be no adversarial process built into this, the way it stands at the moment. You will have a judicial review, but no one putting forward the argument to the judge in a different situation. Now, that is not unheard of; you have that in other situations, but not in relation to a judicial review situation. That is why it is so important, in this sort of situation, for the judge to be able to be hands-on to potentially look at the facts and evidence in front of the judge, for themselves, and make that decision not shackled by any previous assessment that has been made by the Secretary of State.

Suella Fernandes: Do you not think that that will have a negative effect on timeliness and the speed of decisions, in urgent situations when there are real risks, in terms of the quality of decision-making?

Matthew Ryder: It should not do at all. The reason is that it does not have any problem with timeliness in relation to Schedule 1 of PACE. Those can be extremely urgent applications for very sensitive material in the most intense operations. It does not have any problems in relation to Schedule 5 of the Terrorism Act. I could not imagine a more serious situation, where a judge is having to decide on production orders or search orders in relation to terrorism investigations, under Section 39 of the Terrorism Act 2000, which are then being dealt under Schedule 5 of the Act.

Q191 Lord Strasburger: Not only am I not a politician, I am not a lawyer and I have been struggling through the fog of arguments in this area, since this Committee started to sit. It is only just now that I am beginning to see some light at the end of the tunnel. Are you collectively saying that the solution to this whole problem is to strike out the phrase that includes the words "judicial review"?

Peter Carter: Are you asking four lawyers to agree?

Lord Strasburger: I will settle for your individual opinion.

Peter Carter: My opinion is yes.

Martin Chamberlain: Mine is, too. It would be much clearer if you said to the judicial commissioners what standard you are expecting them to apply. You could do that in various ways. One way would be to get rid of the words "judicial review", which imply this shifting spectrum, without telling you where on the spectrum you are.

Matthew Ryder: I would still be inclined towards judicial authorisation by a judge, rather than judicial approval. I certainly think in relation to police cases that "judicial authorisation" would be appropriate. In national security cases, you can have a different discussion, but my preference would be "judicial authorisation", rather than "judicial approval".

Graham Smith: I am a mere IT and internet lawyer. I would not begin to venture an opinion on this.

Lord Strasburger: May I then ask the opposite question? What do those words add to the Bill? What benefit do they bring, if any?

Martin Chamberlain: The suspicion or the worry is that it may be argued by the Government, once this Bill becomes an Act, that what they add is a clear signal or flag to the judicial commissioner that, when you are examining warrants issued by an elected official, you should back off and not question those warrants, unless the decision to issue them was irrational or something close to irrational. Probably "irrational" is the wrong word, because clearly proportionality comes into it but, at the far end of the spectrum, that is the worry. It would be very interesting to hear what the Government say in response to that. If they were to say, very clearly, "That is not what we intend. We intend it to be intensive review", and if they were to say it in a way that could then be subsequently relied on in legal proceedings, that would be very interesting.

Q192 Dr Murrison: We have moved quite a long way towards the double lock. The double lock was a point of some controversy, but has now been accepted by the Government. It is worth just recording that. What you are saying is that you would be happy with the deletion of Clause 19(2), which we heard, for example from Liberty the other day, would materially improve the Bill and the scrutiny available.

May I press you on this five-day period, during which the judicial commissioner would take a view, albeit in the Bill at the moment a rather limited view, on the authorisation that the Secretary of State has given? Do you feel that five days is reasonable, since we have heard from others that it is a very long time for a judge to form a view, particularly since he is likely to be presented with the same sort of material that the Home Secretary deals with, sometimes with a very short timeframe? Indeed, that of course is used as a justification for the Home Secretary dealing with this in what have been characterised as emergency situations, not a judge. May I start? This is something that the Bar Council is particularly concerned about. We can see no justification for that five-day gap. The Secretary of State is a single person. Numerous judicial commissioners can be appointed and, no doubt, will be appointed under the Bill. High Court judges are used to dealing with applications of the utmost urgency.

When there is a need for an urgent application, for example a place of safety order or to prevent somebody being deported from the United Kingdom, I am afraid judges used to be wakened at any time of the day or night and can deal with that matter, as a matter of urgency. There is no reason why a judicial commissioner cannot deal with it as a matter of urgency. For example, a judicial commissioner might be in a position, as the Home Secretary probably might not, under the Bill, to say, "Yes, I authorise this warrant and I want you to come back in 24 hours and I will review my decision and how far it had got". There is provision for that in the Bill, but I can see that practice would develop whereby a judge would make an authorisation that was interim and conditional. I cannot see any reason why five days for a warrant that is potentially unlawful can be justified.

The Chairman: Can you suggest a time?

Peter Carter: I do not think there is any justification for any time, any delay. The delay, if anything, is going to be with the Home Secretary, not with the judicial commissioner.

The Chairman: The issue is one of urgency here, is it not? These are only urgent warrants. We are not talking about the 2,500 to 3,000 warrants that have to go through the various Secretaries of State. We talk about a much smaller number. Would that make a difference in terms of, I do not know, a day afterwards?

Peter Carter: The difficulty about that is that, if it is urgent, you should not prescribe a time limit because, if it is urgent, it must be done immediately.

The Chairman: Indeed, but the issue is if there is a joint authorisation, which there is on a normal warrant, but an urgent one, because of its very nature and what might be happening, the Secretary of State obviously has to authorise. The Bill says you can have up to five days for a judicial commissioner to review that, but you do not think there is any need for any sort of time limit. It depends on the availability of the judicial commissioner, presumably.

Peter Carter: There will be a judicial commissioner available at all times. There should be. It may well be that, if it really is urgent, the Home Secretary or the Secretary of State should be, as it were, a bystanding participant and it should be a single, consolidated process.

Matt Warman: How does that work?

Paul Hudson: The principal decision-maker and authoriser would be the judge. It would be subject to the Home Secretary saying, yes, he or she confirms that it is necessary, so you do it the other way round, in a sense.

The Chairman: To put in my own experience, from when I used to authorise warrants as a Secretary of State—very urgent ones, virtually in the middle of the night or something—you are not going to sit there and have to phone up a judge immediately, when something might have to be decided in minutes, surely.

Peter Carter: That is why I am suggesting that the only reason for having the Home Secretary's decision is this double lock process, is it not? The presumption is that the Home Secretary is a politician who is attuned to security needs and would be the first port of call but, in urgent cases, there is no need for that. The first and only port of call is the judge. If the Home Secretary, having been informed of the information says, "Actually, I disagree", which is highly unlikely, the Home Secretary would then have the power to revoke it.

The Chairman: Why are you suggesting that it should go to the judge before the Home Secretary in an urgent case?

Peter Carter: It is because you then have the consistency of every such warrant having judicial approval.

The Chairman: I understand.

Q193 Bishop of Chester: Is it possible to try to situate this whole discussion between the European culture, which has experienced totalitarian Governments and has a suspicion of government with the history of totalitarian interference, and North America, where there has always been that freedom of the individual and a small state. We are somewhere in between. There is a danger of these wide-ranging powers, which you have identified, being accepted

too easily, hence the need for some sort of robust double lock and a strong culture of judicial independence in the judicial element, I suggest. One of the questions we have raised is if the judges should be appointed by the Prime Minister or by the Judicial Appointments Commission. Should they be appointed for a single term of office, rather than have to submit to reappointment? There are these sorts of questions. Are there other ways of strengthening that culture of independence that you all want to see in the judicial involvement?

Peter Carter: Given the gravity of the kind of situation that is envisaged in this Bill, I would have thought that the appropriate candidates for judicial commissioners are likely to be High Court judges. It may be that it is because we have all gone native in the profession that we see no reason to doubt the integrity and the robustness of people who satisfy the criteria of appointment to the High Court bench. I do think, though, that there is a potential problem of perception, if not reality, if appointment to the judicial commission is by the Prime Minister, rather than by the Judicial Appointments Commission, with consultation with the Lord Chief Justice. That would be more appropriate, rather than it looking like a political appointment.

Bishop of Chester: Would you review after three years, as is proposed, or is it better and more of a culture of independence to appoint for a single longer term?

Peter Carter: I am not particularly bothered. Others may take a different view about that but, if you are appointing somebody of the category I have suggested, either they will be sitting senior judges, in which case after three years they may go back to their normal judicial appointment; or they may have retired, in which case three years would probably be sufficient for them to feel that they have done their job and would quite like to go and do something else. Potentially, it will be quite an onerous job. For somebody in this position, I do not see that there is a problem about the perception of independence from it being a three-year term, in the same way as, for example, for the appointment of the Director of Public Prosecutions, the term is sometimes three years and sometimes five years. Nobody, so far as I am aware, has made any suggestion of lack of independence as a result of a three-year, as opposed to a five-year, term of appointment.

Matthew Ryder: Three years is a short tenure for a judge and it might be that the Judicial Appointments Commission would be well placed to express a view about that sort of time in relation to judicial independence, because they have done some significant thinking on how long tenures should be for judges, to ensure that judges do not feel vulnerable when they next come up for review.

Bishop of Chester: When they appeared before us, the impression given by the judges was that they generally sided with the application. David Pannick's article referred to that benefit of the doubt or margin of discretion or whatever it was he said. I cannot remember the term you used there. One can see that a certain culture of it being normal to go along with the Executive could develop without quite being noticed. I simply put this up for you to demolish. Others who have sat in those seats would certainly have those anxieties.

Peter Carter: All you have to do perhaps is look at the history of the current Investigatory Powers Tribunal and the independence that has shown in standing up against the Government's attempts to keep secret the unlawfulness of some of the conduct, and the tribunal's insistence on making public as much of its judgments as it possibly can.

Martin Chamberlain: I would agree with that. I do not think you need to worry that the people who are appointed to these rules will slip into a culture of doing what the Executive want. What you need to worry about is that judges, in performing their role, will do what they think Parliament has told them to do. If they think Parliament has told them, by use of words like "judicial review", to accord considerable latitude to a constitutionally accountable Minister, then that is what they will do. That is not because they are unable to stand up to the Executive; it is because they are honestly interpreting what you have said to them. If you do not want them to apply considerable latitude, you need to make clear that they are not to do so. If you make that clear, they will do what you say.

Q194 **Victoria Atkins:** Lord Chairman, I am very conscious that I am about to venture into a subject in which you are an expert and I am not, but it is a simple question. Have you taken into account the political sensitivities of Northern Ireland and the way the judiciary is viewed by some, in different parts of that part of the country, when assessing the argument that judges should always come first?

Peter Carter: No.

Martin Chamberlain: I have not either, but I would have thought that, if and to the extent that there are elements of the community in Northern Ireland who have less confidence in the judiciary than perhaps people would have in England and Wales, or Scotland, then one would have thought that those same elements would have a similar lack of confidence or even a greater lack of confidence in members of the Executive.

Dr Murrison: I have a very quick supplementary to that. Do you think then that that is another argument in favour of the Judicial Appointments Commission appointing commissioners, rather than the Prime Minister? If the Prime Minister appoints the judicial commissioners in relation to Northern Ireland, one would also have to involve the First and Deputy First Ministers.

Peter Carter: I first heard that argument raised at a meeting in Portcullis House on the eighth of this month, and it struck me then that I wished I had thought about it before. It seems a very good suggestion.

Q195 **Suella Fernandes:** The Home Secretary will have the power to amend the functions of the judicial commissioners. How do you envisage that power being exercised and what kind of modification might be envisaged?

Matthew Ryder: I do not know is my answer.

Martin Chamberlain: I would say the same. It is very difficult to envisage how it might be exercised. In principle, it could be exercised to add to the functions or to take away from the functions. One potentially worrying use of the power would be if it could be used to alter the test that a judicial commissioner has to apply when considering or reviewing the issue of a warrant. I do not know whether it is intended to use the power or that the power might be used in that way, and it would be an interesting question to get the Government's view on.

Peter Carter: Can I make a suggestion? It seems to me that the power to modify the commissioner's role should be confined to those roles that are not central to the authorisation of warrants and the continuation or renewal of warrants.

The Committee suspended for a Division in the House.

Peter Carter: I am very grateful for that, because it has allowed me to find my place in the notes. The question was about the Home Secretary's power to modify the role of the judicial commissioner, which appears in Clause 177. In the clause as it stands, there are no constraints as to which role or part of the role the Home Secretary can amend. This means that, if you decide to remove the expression "judicial review", the Home Secretary could, by his or her power of amendment, depending on who it was at the time, put it straight back in again, which may not be entirely satisfactory.

This provision, Clause 177, appears in part 8 of the Bill. There are various provisions there that explain or provide particular functions for commissioners, including that the investigatory powers commissioner in Clause 169 must keep under review the exercise by public authorities of statutory functions, and so on. I can understand why that kind of role or function is suitable for amendment, as circumstances and the law change. What I would suggest is that Clause 177 should be amended by adding the words, in subsection (3), "This clause does not apply to any function of the judicial commissioner under parts 1 to 7 of this Act".

Q196 **Victoria Atkins:** I am conscious of the time. Mr Carter, you have written a very helpful paper, on behalf of the Bar Council, regarding legal professional privilege or LPP. Can you help us with any concerns about LPP and investigatory powers and, if there are concerns, how they can be addressed? How would you recommend they be addressed?

Peter Carter: We have concerns, because there is nothing in this Bill that protects legal professional privilege. Legal professional privilege is the privilege of a client to have private communication with a lawyer, to obtain legal advice or for advice and assistance in the course of litigation, whether active or potential. Communications between a lawyer and a client are not all protected by legal professional privilege, and we are not suggesting that all communications between a lawyer and a client should be protected or immune from investigatory powers. For example, the Proceeds of Crime Act makes it quite clear that communications between a lawyer and a client covered by legal professional privilege are immune, but a client asking a lawyer for advice on where the best place is to stash his stolen loot is not. If there was information that led the police or the security services to believe that that conversation was about to take place, then they would be fully entitled, and I would applaud them, for putting in place some of the provisions of this Bill to get evidence that that was taking place.

The difficulty is that, if legal professional privilege, properly so-called, is not recognised as a privilege that needs to be protected, it strikes at the heart of our judicial system, not just the criminal system, but the judicial system. It is the integrity of the judicial system that is one of the guarantors of our state as a democracy.

Imagine the situation if a client in a commercial action were to say to me or one of my colleagues, "I am about to engage on a contract and I need your advice as to the international effects of this. It is with a Russian company. It is very sensitive because I have competitors in other states. Can you assure me that all our communications will be confidential?". Under this Bill, my answer would be, "No, I cannot", because I simply do not know.

The difficulty is that the wording used in Clauses 5 and 65 says that, where a warrant authorises any of the investigatory powers under this Bill, then any action taken in accordance with that warrant is lawful for all purposes. If the warrant authorises the interception or the gathering of data information concerning communications between me and the client, it would be lawful, even though under international law, European law and our historic law, such communications have been immune, as a matter of public interest. The fact that these rights are ancient is neither here nor there; what matters is that they are current and they are important. They are important for the confidence of citizens in the administration of justice.

Interestingly, when David Anderson produced his report, *A Question of Trust*, in a fairly short passage, he described why legal professional privilege is important. He said, if it is apparent that there is no guarantee that legal professional privilege is protected, it will have what he called "a chilling effect" on the relationship between client and lawyers, and their confidence in the entirety of our judicial system.

The Government fight fiercely for its own legal professional privilege, particularly for example when it is engaged in international arbitration. The Belhaj judgment in the Investigatory Powers Tribunal said this, "There was no dispute between the parties", that is between the state and Belhaj, "as to the importance of protecting and preserving the concept of legal and professional privilege". Why, therefore, is that recognised importance not reflected in the Bill? It is in various other statutes, including in the Terrorism Act 2000 and in the Proceeds of Crime Act, as I have already identified, and in the Police and Criminal Evidence Act.

The problem is that there was one clause, in the Regulation of Investigatory Powers Act, Section 27, that used that expression, "lawful for all purposes". The House of Lords by a majority decided that that empowered a warrant to enable the investigating services, police and intelligence services to intercept communications covered by legal professional privilege between a lawyer and a client. In fact, what was uncovered out of that was of precious little significance, but it was a chilling effect. It has had a chilling effect. Those of us who practise sometimes in criminal law realise that what you require is to build up the confidence of a client in order to give robust advice, sometimes advice that they do not want to hear, but they need to hear. If they cannot be confident that the communication is confidential and secret, they will simply say nothing. That does not help anybody or anything.

Why is it not there? It is said by the Home Office that it is all right; it will be in codes of practice. Interestingly, Schedule 6 contains the only reference to something akin to legal professional privilege, and it is in paragraph 4 of Schedule 6. It says, "A code of practice about the obtaining or holding of communications data by virtue of part 3", so it is confined to the powers exercised under part 3, not under any other part, "must include … (b)

provision about particular considerations applicable to any data which relates to a member of a profession which routinely holds legally privileged information", which I assume means lawyers.

There are two things that follow from that. The first is that it recognises, as is evident from the proceedings in the Investigatory Powers Tribunal, that the security services have access to sufficient information to be able to filter those communications that are communications with lawyers, so they know which communications are likely to trigger access to data or communications, which are or the subject matter of which is covered by legal professional privilege. They can do that.

Why is it that the codes of practice under paragraph 4 of Schedule 6 are confined to this particular area under Part 3? The codes of practice or the draft new codes under the Regulation of Investigatory Powers Act also have a provision about legal professional privilege, which does not guarantee the immunity of legally privileged material from access by and disclosure to the agents of the state. It simply says it is a serious consideration, before authorisation is given, not only when it turns out that legally privileged material has been accessed inadvertently, as part of a more general and legitimate operation, but even when it has been specifically targeted.

Whether that will survive a challenge in the European Court of Justice or in Strasbourg, I have my doubts. I am not certain about it, but I have my doubts and I have my doubts because, in international and in regional human rights law, one of the critical basic rights is the right to independent advice or advice from an independent lawyer. Advice from an independent lawyer is going to be worthless if the client and the lawyer believe that everything said is going to be heard by or accessed by the state.

The state, in the cases that are dealt with in the Investigatory Powers Bill, will in most cases, the chances are, face some kind of litigation involving not necessarily the person whose communications are accessed, but somebody else. Eventually, the chances are, the litigation, whether it be criminal or civil, will indeed be between the person whose communications are accessed and the state. The state would not want to be at a disadvantage if another state in international arbitration had access to all its advice. There have been various expressions about the importance of this right over the centuries but, as I say, what matters is its significance now as a right in a democratic society, which is regarded as a guarantee of a democratic principle and a guarantee that citizens are not at a disadvantage in their dealings with the state.

The Chairman: I shall have to curtail things in a second. I am just asking whether your colleagues agree with what you have said on this or have any additional points.

Matthew Ryder: I do not have anything to add.

Martin Chamberlain: Neither do I.

The Chairman: There is no dissention, which is very good. I am going to close the session now. We have, however, a number of questions we would like to put, if that is okay, to all four of you, in writing. I am conscious of your time, but I am also conscious of the fact that I do not particularly want these questions or the answers to them to be missed. If that is okay with

you, we will write to you. We are very grateful. It has been a fascinating sessions and a very important session for this Committee. Thank you so much for coming.

Adam Kinsley, Director of Policy and Public Affairs, Sky (QQ 101-115)

Evidence heard in public Questions 101-115

Oral Evidence

Taken before the Joint Committee

on Wednesday 9 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Lord Henley, Lord Strasburger.

Witness: **Adam Kinsley**, Director of Policy and Public Affairs, Sky, gave evidence.

Q101 The Chairman: A warm welcome to the three of you. Thank you so much for coming along. You represent very significant companies with a lot of relevance for this particular Bill. Apologies to you for starting a bit later, but there was a vote in the House of Commons, which delayed our procedure. I am going to kick off the questions by asking you all to answer the one I am going to ask. If you want to say anything by way of a short general statement, perhaps you would like the opportunity so to do when I have asked the question. Again, welcome to you.

My question is a fairly simple one: how extensively is the Home Office engaged with you with respect to the provisions in the Bill? Perhaps Mr Hughes would start.

Mark Hughes: We have been consulted. We welcome the consultation that we have had. We have had a number of opportunities, and, overall, we are pleased with the level of consultation. There are obviously circumstances where it could be better and we could have done more, but, broadly speaking, it is very different from previous iterations we have had with the Home Office so we are comfortable with the consultation that we have had.

The Chairman: Thank you very much. Mr Kinsley.

Adam Kinsley: Indeed. I would echo that. There has been extensive consultation over the last months and it has been a marked improvement on last time.

The Chairman: Good. Finally, Mr Woolford.

Hugh Woolford: I would echo that. We have had engagement, and we have had high-level engagement both on the legal and operational sides. It is welcome that we are having that engagement.

The Chairman: That is a good start. Lord Butler.

Q102 Lord Butler of Brockwell: Following on from that, you are satisfied with the consultation, but has it led to agreement about what is practicable? Let me elaborate on that while you are thinking about it. This is on the nitty-gritty of how it is done. I am after whether

you think it is practicable to separate communications data from content, or at least the type of communications data you are being asked to retain, whether you are confident that you have the equipment that would enable you to do that, and whether you can give us some idea of what degree of extra costs that would impose on you. I hope that is not too much of a question.

Hugh Woolford: I will kick off and then pass across to my colleagues. I will take it in bits. On how easy it is to separate communications data from content, in the dealings we have had to date we feel that we need more work to get more clarity over what is considered content versus communications data. We need more workshops between the bodies to flesh that out. At the moment there are very high level—

Lord Butler of Brockwell: Excuse me, but does "bodies" mean the Home Office and the providers?

Hugh Woolford: Absolutely, yes. At the moment there are very high-level definitions. You could, for example, say that a route URL for bbc.co.uk is considered communications data, but if you put a "/news" on the end that may be content, so there are nuances—this is the way the Internet is constructed and used—that mean that does not always hold true. There are some general principles in place. We need to move forward and get some more detail in place around some of those nuances and how to handle some of them. That is the first point.

Leading on from that, given that we have not got to the nub of how we would differentiate, the answer is no, to be perfectly honest. We have early discussions going on with regard to some of the equipment or angles that we could look at, but there is a huge piece on volumes, which I am sure we will come to later in the session, that has a massive bearing on the equipment that we need and therefore also the cost.

Adam Kinsley: At this stage, we have to differentiate the conversations and the factsheets we have seen and what we are looking at in the draft Bill. The draft Bill is obviously very high level and it is not sufficient to be able to map across from that and understand exactly what we are going to need to do. By definition, it is going to have to come later in codes of practice and in further discussions. Going back to your question, to be able to differentiate and look at communications data within what are effectively packets of data, there will need to be investment in new types of technology for us to be able to get up to the first slash. The way the Internet is arranged and operated is not simple. We are going to have to look at individual use cases and understand exactly what we will need to do. Hopefully, that answers your question.

Mark Hughes: There are a number of parts to the question. The first is whether or not it is technically feasible to separate content from communications data. The draft Bill usefully defines communications data both from an entity and an event point of view, which is a new set of definitions, as opposed to the previous or existing regime—the RIPA regime—and then content. Technically, it is feasible to separate various parts of the packets; we can deploy tools to do that. The point about that is that, increasingly, especially in the future, with more and more encryption, the ability becomes more limited to take you back to purely an entity level piece of communications data as opposed to richer parts of communication data. That is the first thing.

More broadly, there is a lot of discussion, and has been, about definitions. We have already started talking about them today. It is important to look at definitions in the context of the level of intrusiveness that is the purpose behind the power being sought. That is always the reference point. The definition comes from the level of intrusiveness that is going to impact on our customers and on citizens generally. The definitions are derived from the level of intrusiveness to help bucket, effectively, certain types of data, be it first slash-type data or whatever it may be, to have a way of defining certain types of data. The caution I always put on definitions is that it is not easy to write them down, and we can see that right across the Bill, but with the additional checks and balances put into the draft Bill around legal oversight stuff, there is the possibility to refer back to the level of intrusiveness. Where the definition in the draft Bill might not be sufficient at the moment, there is the possibility through oversight to question that.

I think your next point was about whether or not the equipment exists. Yes, it does. There are various technologies available to us, although they are limited by the way in which the traffic is sampled, and there are many considerations around that. Indeed, some of the Bill, especially in the area of Internet connection records, which are new data that we have never collected before for that purpose, means that we will have to deploy new equipment to comply with the legislation as it is drafted. That comes at a cost. Clearly, there are two things about costs that concern us. First, it is not clear in the Bill at the moment that we will be eligible to recover all our costs, and we think that is important for two reasons. First, the mere fact of defining how much something will cost to meet a certain type of power will help to limit and frame the level of intrusiveness. In other words, an open-ended view of what something could cost could be problematic in the sense that capability could be stood up, which could cost a lot. Therefore, a proportionality check comes in through ensuring that it is clear that costs will have to be met. Secondly, clearly, if the cost is not met in that way, it will have to be found in some other way. There will be additional costs and we certainly have some views on some of the calculations—perhaps we might talk about that later on.

Lord Butler of Brockwell: When agreement on definition is reached, how do you envisage that it will be expressed in statutory form, or would it be expressed in statutory form? Would it be by a statutory instrument or will further amendments to the Bill be necessary?

Mark Hughes: This process, through scrutiny, is in part helping to tidy it up. There is, I believe, much more work to be done to ensure that we get tighter definitions where we can. Equally, as in my previous point, we have to ensure that the oversight regime allows us the ability to discuss that. More specifically, to answer your question, the codes of practice, which we look to see before the publication of the final Bill, will go some way to clarifying a lot, as well as the oversight instruments that exist in the draft legislation, which will allow us, if we are not comfortable with that, to visit it with the appropriate authority.

Q103 Lord Strasburger: Gentlemen, you have mentioned encryption as being a complicating factor. We have also heard in previous sessions that the way the Internet is increasingly being used—for example, with a Facebook page—is as a smorgasbord of content and data, and that it may be impossible to separate them automatically. I doubt that you would fancy doing it manually. How are you going to cope with that problem?

Adam Kinsley: You have put your finger on the nub of the technology challenge. When you are requesting a page within Facebook, facebook.com/spurs, or something like that, you are going to get lots of different content delivered: you are going to get the league table, the Harry Kane goal or something like that—lots of data. We need technology to analyse all of that, match it all up and work out which bit is the first slash. It is a big technology challenge. As Mark says, it is not impossible but it is very expensive.

Lord Strasburger: Thank you.

Q104 **Dr Andrew Murrison:** Obviously, there is some urgency to all this because the Home Office would rather like to get cracking with gathering the information that it says is necessary to safeguard security and deal with serious crime. I am interested to know from you how long you think it is going to take, given the technological challenges that you pose, to get to that first slash point.

Hugh Woolford: We have put some thought into the timescales. As long as the necessary discussions and detail were worked through, we feel that we could probably start in 2017, with earliest deployments in 2018, depending on the requests and the scale. Those are the sorts of timescales that we would potentially be working to.

Dr Andrew Murrison: That sounds quite a long timeframe to me. Does that match the level of patience that you perceive in your dealings with the Home Office, or is it disappointed by that?

Hugh Woolford: I honestly cannot comment on that. Those are the timescales that we have in mind. That is currently where our heads are.

Dr Andrew Murrison: I have to say that the definitions on the face of the Bill confuse me; I suspect that they will probably be rather clearer to you since you are in this particular business. I have heard from you already that you value the improved definitions, particularly those in Clause 193, which I guess is what you are referring to when talking about entity data and events data, but I am also hearing that you expect further clarification by way of codes of practice. Where do you think we are at the moment with the definitions? Where on a Likert scale of zero to 10—where zero is completely useless and 10 is perfection—do you think we are at the moment?

Adam Kinsley: I am not sure that the intention is for us to be able to deliver any capability based on the face of the Bill alone. As it stands, it is pretty close to zero, I would say. We absolutely need more detail to be able to deliver. I am not sure it was the Home Office's intention to be able to deliver based on the definitions on the face of the Bill, but that is obviously a decision for Parliament—how much goes on the face of the Bill, how much goes into codes of conduct.

Mark Hughes: There has been a lot of work to help to clarify a number of the definitions in the Bill. In the Internet connection records space, for example, it is difficult for us to comment because we are not defining the purpose for which it is intended. Therefore, by its very nature, I am not in a position to comment. There has been a lot of work. As we have already said, there needs to be more work and the codes of practice should support that.

Adam Kinsley: I should qualify my comments. I was answering in relation to Internet connection records primarily.

Hugh Woolford: I would echo that.

Q105 **Mr David Hanson:** Page 25 of the draft Bill, regarding Internet connection records, says helpfully: "A kind of communications data, an ICR is a record of the Internet services a specific devices has connected to, such as a website or an instant messaging application. It is captured by the company providing access to the Internet". Is that your understanding of what an Internet connection record is?

Hugh Woolford: Today we do not have anything like an Internet connection record. This is something that is completely new for us, and I have looked at previous Bills. From a business point of view, there is no need for us to capture any of this information. We do not have what could be classed as an Internet connection record.

Mr David Hanson: I am a layman here, so tell me how hard it is to collect one of those, to establish it.

Mark Hughes: On the face of it, it sounds like a relatively straightforward thing to do. In some respects, the Bill goes on to define the purposes for which they are being collected, and three purposes are outlined. They are obviously around the person, illegal content and the service, broadly speaking. It helps as well when you combine the two things; you take the initial definition and the purposes that are in the draft Bill, and that has given us a route to analyse what would need to be collected—as Hugh said, it is not something that we collect today—to fulfil that definition and then have data available if that were to be the case for that purpose. You would have to look at quite a lot of data to be able to achieve that.

Adam Kinsley: If you think about what a CSP would be required to retain at the moment, essentially you may be given an IP address that would be applicable to your computer for potentially up to a week and that would get recorded once. There are a couple of bits of data that would be recorded for about a week. In what the Bill is seeking to do, first of all you would have to analyse all your Internet sessions in that week—in fact, throughout the whole year—which would obviously be quite a lot; in the Facebook example we used earlier, just one request to a Facebook page will come back with lots of information within it that needs to be matched. You need to analyse all that, match it all up and then retain the bit that the Bill will ultimately end up with. The magnitude of data collected that would be processed would be massively more and the magnitude of data that would then be retained would be tenfold, a hundredfold more than we collect today.

Q106 **Mr David Hanson:** At the moment we are considering the draft Bill; it is going to go through the House of Commons and the House of Lords and be law by September or October next year. How long is it going to take you to establish the mechanisms? How much is it going to cost you to establish the mechanisms? Who do you think is going to pay for this? Is it the taxpayer, as in all of us? Is it you or a mixture of both? If so, what is the mixture? Is it practicable? Is it going to do what it says on the tin? We need to get a flavour of this from you.

Mark Hughes: Let me go through a number of those things. There is a spectrum of options available on Internet connection records in terms of the amount of coverage. The Home

Office has consulted us and we have had a pamphlet that has been issued about Internet connection records, with some view of costings. We have obviously done work based on the assumptions. The assumptions from the Home Office are that it wants as broad a coverage as possible to achieve this, which is going to be costly. We have worked up some assumptions and indicative costing.

Mr David Hanson: Are you able to share that with us or not?

Mark Hughes: Yes. The publicly stated figure, I think, from the Home Office is that it has set aside £174 million for this. We have worked out that for us alone—I cannot comment for others around the table or others in the industry—to fulfil the assumptions that we have been given will cost us tens of millions, so the lion's share of that £174 million would be for us alone. How others would do it depends on how they manage and architect their networks. We have looked at it. As to the implementation time that it would take, again it depends: there are some things where extant capability could be used to gain some coverage relatively quickly, but to fulfil the assumptions we have been in dialogue with the Home Office on, it would take longer to deploy equipment comprehensively across our network—deep packet inspection equipment—to be able to generate the data to then have them retained to comply with the legislation.

Hugh Woolford: On costs, we broadly agree. Our teams have had a look at the high-level information we have and think similarly—tens of millions. I would love to give you an exact figure. We are not saying it cannot be done. Anything can be done in this space with enough time and money. We have a broad set of requirements, but to enable us to move forward we need to bring some more specificity to those so that we can start giving more accurate estimations of costs and time. Depending on how much you are trying to capture and across what frequency, one big piece of it is how much of whatever the equipment is you might need to deploy; therefore, you need to find space, power and places to host it all. It is no mean feat. This Bill potentially could look at all of us having almost to mirror our entire network's traffic to enable us to filter it. It is a huge undertaking.

Mark Hughes: You asked about costs. We believe quite strongly that the costs should be met by the Home Office—that we should seek to have 100% of our costs in this space reimbursed. The reason is that, if you start from the basis that there is no cap on the cost, you may end up with a disproportionate technical solution that could be overintrusive, so the cost in itself will help bound the solutions.

Mr David Hanson: To help the laymen and women among us, if the taxpayer chose to support the cost of developing this scheme, do you think £170 million is a reasonable estimate, given what you have said in your previous answers, or not?

Mark Hughes: Based upon the assumptions we have seen, from our point of view, yes, because it would cover what we need to do, but if you aggregate it across the industry—

Mr David Hanson: It is not just you, is it?

Mark Hughes: Absolutely not.

Mr David Hanson: Otherwise the terrorists and criminals would not use BT; they would be using something else, would they not? So it cannot just be you.

Mark Hughes: Indeed. There are obviously other ways in which other networks are architected. There are, though, other assumptions. You could use less sampling of traffic, which would perhaps give less coverage, but there would be a trade-off in the amount of cost.

Q107 **Mr David Hanson:** This is the final question from me, Lord Chairman. Let us look two or three years ahead to when this has all been done, someone has paid for it, it is all available and the aspirations on page 25—of the Government and you—have been met. What do you think about how the Government access that material? Are there sufficient safeguards in the Bill for single point of contact officers? Are there sufficient safeguards in the Bill for access by the security and police forces via the Home Secretary, or whoever, in the Bill?

Mark Hughes: On that point, the Bill is clear that there are three purposes under which the data we are talking about, the Internet connection records, can be disclosed. That is fine. However, there are further parts of the Bill that refer to forward-looking capability. We believe, going back to one of the points I made earlier, that that potentially changes the intrusiveness before the data are disclosed and would, in our view, require a check against the level of intrusiveness that it would incur and a referral back to the legal oversight to ensure that we were not stepping outside the intention that was originally conceived in the three purposes.

Hugh Woolford: Can I raise an item on the emergency single point of contact? One of the items that is suggested is emergency SPOCs. We feel that could give rise to an ability to breach the system. In an hour of need—the golden hour—how are you going to validate who is asking for the information? It would be better if the normal SPOCs—if "normal" is the right word—were to provide cover so that there was a single list of authorised people who can ask for it. Having an emergency, somebody ringing up or contacting and saying, "We need this because someone's life is in danger", gives an opportunity for that to be abused. We feel it is better if the SPOCs cover each other. That is an area that we would like to have looked at.

Mr David Hanson: Apart from that, it is all going well.

Q108 **Stuart C McDonald:** I have one short supplementary on these points. One or two witnesses made reference to a similar scheme that was operated in Denmark. Is that something you guys have looked at? What were the similarities and differences? Is there anything that can be learnt from what happened there?

Hugh Woolford: No, I have not looked at that, I am afraid.

Mark Hughes: I understand that the system in Denmark has failed because the software has not worked. That is what I am led to believe.

Stuart C McDonald: Is there anything we can learn from that? Is the scheme that you are being asked to implement similar?

Mark Hughes: I am not familiar with the ins and outs of the detail of it; I am just aware of the headline. Through the consultation and the technical feasibility that we have done, we believe there are technical solutions that we can put in place—subject to the Technical Advisory Board confirming that. They would perhaps draw on that Danish experience, but we have to be careful that we implement them properly. There is no reason why, if we have the right solution and we implement it properly, it will not work.

Q109 Lord Butler of Brockwell: I have one supplementary. Could you break down the £174 million between the one-off cost of getting the right equipment and then the recurrent cost of maintaining it?

Mark Hughes: The capital investment—the deep packet inspection-type equipment that needs to be put in place—has to be factored against the very strong growth, or fast growth, in bandwidth over the period. The Home Office looked at this over 10 years. Then there is obviously the ongoing cost of maintenance, but also primarily storage. There is an initial upfront investment, but storage is the thing that is going to take up a fairly big chunk of that cost.

Lord Butler of Brockwell: Can you give us an indication of how much of the figure you gave is the once-and-for-all cost?

Mark Hughes: I do not have the figures off the top of my head, but it is skewed quite heavily towards making sure that there is storage. It is not to say that the initial investment is not insignificant, but the storage is also a significant part of it.

Lord Butler of Brockwell: We are talking about £174 million per year, are we?

Mark Hughes: No. From my own point of view—BT's point of view—it is a fraction, so to speak, of that, but we look at it over a time period. There is an initial upfront investment and thereafter the storage.

Adam Kinsley: It is possibly worth adding that, whereas in the previous regime data growth did not matter that much, in this regime it very much would and data growth is running at doubling every 18 months or so. That needs to be factored into any equation.

Q110 Suella Fernandes: It will be a challenge to maintain the security, but to assess the challenge that is going to be presented by the Bill, what in a technical capacity is available to you to reassure the public on the security of data retention?

Hugh Woolford: We have discussed this. We will obviously look to work with the government security advisers to ensure that any processes and systems that we put in place to meet this Bill would meet those requirements and then regular auditing of them. That is the best way we think we could assure that everything was secure and in place. As a matter of course, you have to create a culture and a process around it that brings rigour.

Suella Fernandes: What is your assessment of the effectiveness of things like firewalls and personal vetting systems, and how realistic are they as tools to expand on?

Mark Hughes: It is about creating a layered approach to defence, ensuring that the controls are proportionate, given the sensitivity of the data. We are talking about collecting data for the first time—data we have not collected before—and the key is to ensure that our customers and their rights are protected. That data has to be looked after very carefully, so we have to have a commensurate security wrap around them that takes account of our customers' human rights and indeed their privacy as well so that we ensure that we maintain and safeguard that.

Adam Kinsley: We currently work with the Government on standards, but it could benefit from being more joined up on the Government's side. The Home Office, the ICO and the National Technical Assistance Centre having a single set of standards that we could build to would make a lot of sense.

Mark Hughes: We see a key role for the proposed Investigatory Powers Commissioner and its office being responsible. Clearly the Information Commissioner's Office has a role as well, but it would be useful to us in this context to have a joint agreement between the Investigatory Powers Commissioner and the Information Commissioner's Office, perhaps through a memorandum of understanding. We would rather have the Investigatory Powers Commissioner as the authority to which we could go to seek advice to ensure that we were meeting the correct standards to safeguard that information.

Suella Fernandes: Of course the Information Commissioner will have an auditing power over the security of the systems. How would you describe the appropriate level of engagement with the Information Commissioner?

Adam Kinsley: In the past we obviously had normal business interaction with the Information Commissioner. It seems to us that with this opportunity, when we are creating a new commissioner for these purposes, it might make more sense to bring all of that under one roof; if we are looking at the security of these specific systems, now might be the time to look at having it all under the Investigatory Powers Commissioner rather than two separate organisations.

Hugh Woolford: We absolutely echo that. It brings clarity and conciseness. That is our absolute view. We would rather have it brought under one, definitely.

Q111 Suella Fernandes: This is my last question. There is some suggestion of introducing a criminal offence for data breach by communication service providers. Do you think that is going too far? Do you think it could act as an incentive?

Mark Hughes: We take the privacy and security of our customers' data extremely seriously. As is well reported in many parts of the press, it is something that we take so seriously that we do not necessarily see criminal powers as necessary. We already take it extremely seriously and we believe that the sanction if something goes wrong is that one can quite clearly see the consequences almost on a daily basis.

Hugh Woolford: That is more or less what I was going to say.

Q112 Stuart C McDonald: I want to ask about request filters. What is your understanding of how a request filter would work, and what concerns, if any, do you have regarding its operation?

Hugh Woolford: We have had engagement on the request filter. It is not specified as such in the draft of the Bill. We understand that information would be asked for, we would pass it into a filter and then ensure that only the specific information is passed back, so it stops massive information coming back. We have a few specifics, but the principle is purely at high level, as a concept more than anything else, at the moment. Without wishing to sound like a broken record, this is something else that definitely needs to be looked at and worked through in more detail. One thing that we do not want to do is to become data analysers of information.

Mark Hughes: We understand that it is for the Home Office to design and build the request filter and that it will sit between us as a communication service provider and the law enforcement agency. That is how we see that it will work, but, as Hugh said, there is more to be done. It will use an algorithm essentially to limit the data that are disclosed or presented to the law enforcement officer, who is obviously authorised to see the data, so it limits the data just to those who are necessary to that question.

Stuart C McDonald: Does the information you have just given arise from discussions you have had with the Home Office?

Mark Hughes: It is what I understand from discussions we have had with the Home Office. We have a concern, once the system is effective and in place, that there could be a situation where lots of questions are asked and continue to be asked of it, so our view is that more work needs to be done through consultation to ensure that we—again, going back to my previous point about intrusiveness—level up if multiple questions lead to a point where it is becoming overintrusive. An important principle for us throughout the Bill is that we should always level up to the highest level of authority when we think intrusiveness is becoming greater than was originally intended.

Lord Strasburger: There is a view abroad that the provision in the draft Bill for the request filter is not much more than a placeholder for the Home Office to return to this in the fullness of time and, effectively, write its own cheque on what this will deliver. From what you are saying, it is not giving you very much detail about what this is to do. Is that a possibility?

Adam Kinsley: I would not like to comment on whether it is a possibility. As I understand it, the request filter is there to limit and to be a protection against the flows of information. I would not want to speculate where it might go. We certainly have not seen—

Lord Strasburger: The fact is we do not know where it is going.

Adam Kinsley: The fact is we have read factsheets and had discussions about the concept.

Mark Hughes: The thrust of it is that it is about limiting the amount of data that will ultimately be disclosed to answer a particular question, which is important from a proportionality point of view.

Q113 Lord Henley: Can I turn to the maintenance of technical capability and what is proposed in Clause 189 of the Bill, which you will be aware of? As you know, the Secretary of State will be able to impose various obligations on relevant operators and that will take the form of a technical capability notice, and she will obviously have to consult about that. What are your views on the ability of the Secretary of State to impose a technical capability notice? How do you think your customers are going to react if they are aware that the power exists but they will not be aware of any specific imposition, because that will not be disclosed?

Mark Hughes: There are a few points on technical capability notices. The first one is that we believe quite strongly that the Bill should be clearer in its definition of the fact that the capability notice should be limited to public telecommunications services. At the moment, the definition is not clear, and we are quite clear that it should not extend to private services; it should be limited specifically to public telecommunications services. The second point is that the notice should be served on the provider who is closest to where the information can be provided from. You used the example of Facebook earlier on. That is a matter for Facebook to deal with and the technical capability notice should be directed at that organisation, if indeed it is the closest to the information, which is its information. It should be served, therefore, on those closest to the place where the information is maintained. Beyond that, the existence of a technical capability notice, as in the draft Bill, formulated through the Technical Advisory Board, is good. That there is consultation and oversight that needs to happen before it can be issued is a positive thing.

Lord Henley: What about the views of your customers?

Hugh Woolford: It is definitely not my place to comment on what the views of our customers may or may not be, I am afraid. We are concerned about that, absolutely, but at the moment we have not consulted with them or asked them, so it is wrong for me to offer up an opinion.

Mark Hughes: It is not the technical capability notice per se; in entirety, all the notices that come from this, those beyond the technical capability notices, are something that our customers need to be aware of. Transparency is one of the reasons for this new Bill.

Q114 Lord Henley: You mentioned oversight and the importance of that, and it was partly dealt with in earlier questions from Ms Fernandes about the Information Commissioner. I forget who answered this and whether it is your collective view, but I got the impression that you would like the proposed Investigatory Powers Commissioner and the Information Commissioner to be one—to be merged.

Hugh Woolford: Yes.

Mark Hughes: I am not advocating a merger, but for the purposes of the Bill we feel that for the Investigatory Powers Commissioner there should perhaps be some memorandum of understanding with the Information Commissioner. As I understand it, the Information Commissioner has many other jobs to do beyond this. There is no merging of the two, but just for the purposes of this Bill it would be useful to have one place to go to. We are all agreed that it is the Investigatory Powers Commissioner.

Lord Henley: Because the Information Commissioner is doing other things, in other words, he would delegate his bit of it.

Adam Kinsley: I am not sure how you would bring it into effect. If what we are talking about is security oversight of systems designed to fulfil the obligations in the Bill, it seems that the specialist commissioner would be best placed to carry out that function.

Mark Hughes: Can I make one more point about the technical capability notice? Following on from the point about those providing the service, and that the one closest to the service should be the focus of the Bill or any action that is served, it is not appropriate, we believe, for a network provider to be used as a one-stop shop. It is absolutely important that we process and manage data on behalf of our customers. Where that data is processed by another organisation, it should be subject to the technical capability notices.

Hugh Woolford: Adding to that, if I may, the retention and storage of third-party data is something we are also concerned about, linked with that whole piece. We do not want to be seen as that one-stop shop and asked to retain and store data for third parties that are not to do with our core business or core customer groups.

Lord Strasburger: How do you feel about GCHQ engaging in covert bulk network interference against your networks?

Adam Kinsley: I personally do not have a view on that. That is a matter for you guys to consider.

Q115 **Lord Strasburger:** My question is: how do you feel about your networks being amended covertly by GCHQ and the risks associated with that?

Mark Hughes: It is important to note that any power in the Bill that is instigated in that particular arena has to be proportionate and has to have the right checks and balances over the amount of intrusiveness. The oversight has to take account of the fact that, by their very nature, those types of powers are quite intrusive, so the levelling-up process of the oversight needs to be such that there is full legal oversight.

Lord Strasburger: My question was about the risk to your networks. That is what I was asking about.

Mark Hughes: We are certainly not in favour of anything that would undermine the integrity of our networks.

The Chairman: Gentlemen, we are very grateful to all three of you. Thank you very much for coming along and giving evidence to us.

Graham Smith, Partner at Bird & Bird LLP (QQ 186-196)

Evidence heard in public Questions 186-196

Oral Evidence

Taken before the Joint Committee

on Wednesday 16 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Lord Butler of Brockwell, Bishop of Chester, Lord Strasburger.

Witness: **Graham Smith**, Partner at Bird & Bird LLP**,** gave evidence.

Q186 **The Chairman:** A very good evening to you. I am sorry that we are a little later than we thought, but we have had a couple of fascinating sessions. I have not the slightest doubt that this will be equally fascinating. You are all most welcome to the Committee. As you know, in these situations different Members of the Committee will ask different questions, but I am going to ask a very general one, which perhaps gives you an opportunity to make a general comment on the Bill that the Committee is considering, if you wish to. Aside from the new powers on the retention of internet connection records, in your view, does the draft Bill consolidate existing powers or extend them? In answering me, if you wish to make any more general comments, please do so.

Matthew Ryder: The answer to that question depends slightly on, when you talk about extending the powers, whether you mean extending what the security services and the authorities are already doing and what they say is authorised, or what others would say is currently authorised under the existing legislation. There is a dispute and lots of litigation about what is or is not currently authorised under the existing legislation.

My view would be that there are a large number of new powers that are not properly authorised within existing legislation. Just to go through them with headlines, in Part 1 of the Bill, thematic warrants are allowed in relation to Clause 13. There is not a thematic warrant provision for targeted surveillance and targeted interception within RIPA. I know that the Government say that, if you cross-reference Section 8(1) with Section 81, you can find group surveillance as part of targeting but, realistically, thematic warrants are something new, and the idea that you could target people as groups by their activity is something new in part 1 of the Bill. It is important because, conceptually, it is anathema to the existing culture of surveillance that has been going since the 18th century in this country. If we are to move in that direction, it needs an informed parliamentary debate about it, to decide if we want to go in that direction.

Secondly, mass surveillance or bulk interception—whatever you want to call it—under Part 2 of the Bill is essentially something new. I understand—I was involved in the case and litigated the case in the IPT last year—that the Government say that bulk interception or

bulk collection is permitted under Section 8(4), but there is a dispute about that. There is a case on its way to Strasbourg. It has been communicated in Strasbourg. There are many of us who would say that it was not set out very clearly, if it was permitted at all, in RIPA.

Part 5, on equipment interference, is really new. It has really emerged only since the draft code of practice was published in February 2015 in response to ongoing litigation. It turns out that the Government's position on the existing power is that it is a very broad power, under Section 5 of the Intelligence Services Act, combined with the draft code that they published on the door of the court in February 2015, so equipment interference is new. It is a very significant power that requires a lot of scrutiny and debate.

Part 7, on bulk data sets, is essentially new, has not been regulated before and is not in the existing legislation in any meaningful way. The power to have access to bulk data sets and how they would be defined is something new.

I missed Chapter 2 of Part 6 on bulk communications data acquisition. That is essentially new. In other words, the large collection of communications data in bulk is something that was not clear from any legislation before. That is essentially being regulated for the first time, under this Bill.

Finally, it is arguable—this is more debateable—that Clause 189, which is the clause that has tech companies particularly concerned, is if not new then certainly of new significance, because it requires telecommunications service providers to maintain their capabilities and combines that maintenance requirement that existed in RIPA with a new definition of a telecommunications service and those who are providing that service. It is broadened out by Clause 193(12) to those who are allowing those communications. That means that those companies that simply have communications apps that facilitate communications through the internet, such as Facebook, Apple or those sorts of companies, may be caught in a way of maintaining their capability that they had not imagined before. That opens up the question of whether encryption is engaged in relation to that issue and, if it is not in the Bill as it stands, in due course whether that is a concern. In summary, there is quite a lot here that is very new and these powers are important. They are significant and, therefore, because they are new, they would require debate.

Martin Chamberlain: That was a very comprehensive answer that enables me to be much briefer. The answer to whether and to what extent the Bill contains new powers is very difficult, for this reason. In the run-up to the tabling of the Bill a number of things that nobody knew the agencies were doing, they were revealed to be doing under the existing powers. There has not been time for some of the things that we have very recently found out the agencies are doing to be tested in legal proceedings. I am thinking there particularly about the use of the extended definition in Section 80 of RIPA effectively to enable thematic warrants to be issued, and the use of Section 94 of the Telecommunications Act 1984, which is something we found out about for the first time in the immediate run-up to the tabling of this Bill. As to whether those activities that we now know have been undertaken by the agencies are lawful under RIPA, the answer is that it has not been tested and so it is very difficult to know.

Generally speaking, whether the Bill confers new powers is, with respect, not a terribly helpful question. One of the important purposes of this Bill is to get a democratic mandate

for things that have not yet had a democratic mandate. Whatever you might say is the correct judicial interpretation of some of the old powers, certainly it can be said, without any doubt, that quite a lot of the things in this Bill are things that nobody in these Houses of Parliament has examined the justification for, to date. Are they new powers? One can debate that. The courts have not had the opportunity to debate it, in many instances. They certainly are new in the sense that they have not had a democratic mandate, in many cases.

Peter Carter: Needless to say, I agree with all that has been said, so I shall be even shorter, I think. This Bill is important, because it enables the democratic process to take control of what has hitherto, to a large extent, been a hidden exercise of what is known as a prerogative. It is about time that the prerogative powers were brought to heel and this is a good way of doing it.

Insofar as this Bill brings within the ambit of the law practices that hitherto have either been questionable or possibly outside the law, there is a huge amount to commend it. Only if the kind of activities that this Bill encompasses are subject to law and lawful control, and therefore lawful monitoring, can it be said that these powers are being exercised in a truly democratic way. We need the powers in this Bill, to some extent or another, to combat serious crime, terrorism and actions against the state. The exact extent is a matter for political debate, as well as legal debate.

One of the problems and one of the ways in which the current drafting of the Bill, potentially and exponentially, will extend the powers is in the definitions clause, Clause 195, which includes a definition of data. As Matthew has said, one of the things that appears to be an extended power is the bulk acquisition of data. Data is defined in Clause 195 as including any information that is not data. Therein lies a problem.

Graham Smith: I am going to be slightly longer. I have identified quite a few new aspects that are potentially new powers in this. First, although the question caveats out internet connection records, we do need to understand that, when one looks at Clause 71, which is the power to issue data retention notices, and one compares it with the existing data retention powers in DRIPA, as amended by the Counter-Terrorism and Security Act of 2015, and if one adds internet connection records to that, Clause 71 still goes far beyond adding internet connection records to the existing data retention powers.

Although this has been presented as something to enable the retention of internet connection records, it goes far beyond that in five or six different ways. Perhaps most significantly, the existing DRIPA powers are restricted to a few types of human-to-human communication—internet email, internet access and internet telephony. This would catch all the background activities on my smartphone that happen when it is sitting by my bedside when I am asleep, when I am away from it, whether it is receiving notifications, getting software updates or anything of that sort. It would capture and cover any machine-to-machine communication, which if you look forward to the internet of things would cover my connected home thermostat or my car checking if it needs a software update. Essentially, anything connected to the internet or indeed any other type of network would fall within Clause 71. It now applies to private services and systems, as well as public, and of course the power to require data to be generated for retention, not just retained, is completely new. The previous limitation to retaining data generated or processed within

the UK has been removed, so Clause 71 is very much broader than one might think by just referring to internet connection records.

Other new and extended powers are technical capability notices, under Clause 189. At the moment, under RIPA Section 12, capability notices can be given to support interception warrants and nothing else. Section 189 will apply also to all the new types of thematic, targeted and bulk warrants, under Parts 5 and 6, and will also apply to support the acquisition of communications data under Part 3. All of that is new.

In bulk interception, there is a new power. I call it a new power, but it comes as a result of the warrantry definitions; however, there is effectively a new power to extract related communications data from content and to treat it as related communications data. For instance, if I send you an email saying, "Here is somebody's email address", that is part of the content of my email, but the email address can be extracted from the content and then treated as related communications data. That is very significant, because most of the restrictions on examination of content do not apply to related communications data, so it is very significant. That is replicated as well in the new bulk acquisition and equipment interference powers, which talk about equipment data, which is more or less equivalent to related communications data. There is the power to extract equipment data from the content that is acquired in that way.

Lastly, there is the extension generally through the knock-on effects of the expansion of the definition of telecommunications operators in the draft Bill.

The Chairman: Thank you so much. They were some very useful answers.

Q187 Matt Warman: Given that we cannot agree on what is meant by new, I slightly hesitate to ask this. The Committee has been blessed with lots of different interpretations of what judicial review will mean in the context of this Bill. What do you think judicial review terms would mean, as far as the authorisation of warrants would go, in this new Bill?

Martin Chamberlain: You have just heard from David Davis about Lord Pannick's article in the *Times*, where he suggested that, in this kind of context, the judges would be applying a high intensity of review. One can explain it in this way: whenever a judge is applying a judicial review standard, there is a spectrum of different types of intensity of review. At one end of the spectrum, there is very light-touch review, which David Davis accurately described as, "Don't touch it unless it's totally barmy". Then at the other end of the spectrum, there is a real rolling up of the sleeves, getting into the detailed kind of review, where the judge comes close to substituting his or her own judgment for that of the ministerial decision-maker.

Practically any judicial review practitioner will tell you that, in practically any judicial review case, a key point of contention between the parties is where on the spectrum that case lies. Is it a light-touch case, is it an intensive-review case or is it somewhere in between? David Pannick's article in the *Times* suggests that this would be an intensive review kind of case. David Pannick is generally right about most things, but I would venture to suggest that you need to apply a bit of caution to whether that is correct in this context. Certainly it is true that a warrant authorising interception involves an invasion of someone's privacy,

but it does not involve the kind of restriction of liberty that you see in, for example, a control order case or a TPIM.

The Committee suspended for a Division in the House.

Matt Warman: You were in full flow on what judicial review is likely to look like in this context.

Martin Chamberlain: I have explained that there is a spectrum in judicial review, in terms of intensity of review, with very light-touch review at one end and high-intensity review at the other. David Pannick thinks that, because of the privacy context, we would be in the high-intensity part of the spectrum. I question really whether that is correct. The reason I question it is this: the matters under review, under Clause 19, are whether the warrant is necessary and whether the conduct authorised is proportionate. If you just concentrate on that second question, you are asking yourself the question as a judge reviewing this warrant whether the national security benefit to be derived from the warrant is proportionate to the intrusion into privacy that it involves. That is, to my mind, typically the kind of question on which judges will give a great deal of what used to be called deference—some of the later judgments deprecate that term, but leeway or latitude, however you want to put it—to the elected Minister. That is what would normally happen in judicial review. There is a House of Lords case called *Rahman* that makes that point. Where you are looking at proportionality assessments by a Minister who is accountable to Parliament, you apply a very light-touch review.

The touchstone, if you really wanted to get an interesting answer to this question of where on the spectrum it lies, is to ask someone from the Government what they think and see if they would be willing to give the kind of parliamentary statement that could be relied on in subsequent legal proceedings, to say that what they meant by judicial review was intensive review. I doubt whether you would get them to say that, because I suspect they would want to reserve the position to argue in front of the commissioners that it was a light-touch review that was intended.

Peter Carter: I hope Lord Pannick is correct, but I also fear that it is so uncertain that he may not be. This is not an area in which uncertainty can possibly be allowed to be sustained. One of the problems about judicial review is a problem that was created by Lord Judge last year because, in a decision called *Regina v L*, a decision in the Court of the Appeal in which he gave the judgment, L was somebody who as a young woman who had been trafficked for exploitation. The question was whether it was right that she should be prosecuted for an offence that she committed as a result of her exploitation, which we would now call modern slavery. The issue was what test is to be applied to the decision of the Crown Prosecution Service to proceed with her prosecution, even though all the circumstances demonstrated that she was a victim of exploitation. The test to be applied is one of judicial review.

There was the kind of discussion that we have heard about: on the one side this; on the one side that. Lord Judge said that we are going to apply in this case a test that is not the conventional judicial review; it is something different from that. The difficulty was that he did not say what it was. I do not know anybody at the Bar, who practises in that area of

law, who understands what the test with which we are left in that area of law is. What I suggest is that the simplest way of removing this ambiguity is to suggest an amendment that you simply delete the words about judicial review.

May I go back to the stage about how the judicial commissioners will consider this? It starts off with reviewing what? A decision by the Secretary of State. Normal judicial review is a review of a decision and the reasons for that decision. Are those reasons irrational or are they rational? Do they include considerations that are immaterial or are they centred on considerations that are central to the issue in point? I do not think there is any provision in this Bill for the Secretary of State to give reasons for his or her decision. The judicial commissioner will not be reviewing reasoned decision. The judicial commissioner will be reviewing the decision and, therefore, ought to be reconsidering from scratch whether or not it is appropriate to authorise this warrant and doing so by applying the test of necessity and proportionality.

There is one slight twist about this because, by Clause 169(5) of the Bill, "In exercising functions under this Act, a Judicial Commissioner must not act in a way which is contrary to the public interest or prejudicial to … (a) national security, (b) the prevention or detection of serious crime, or (c) the economic well-being of the United Kingdom". I cannot imagine for a moment that any judge or judicial commissioner would act in a way that is contrary to the public interest, but who is to determine and who is to assist the judicial commissioner on what is national security, what is in the economic wellbeing of the United Kingdom, particularly if the judicial commissioner is not assisted by reasoning from the Secretary of State? If there is to be reasoning from the Secretary of State, how long is this process to take and why not simply remove the Secretary of State from the process?

Matthew Ryder: May I just make two very short points on this? The first one is that the role of the judge in judicial review, when it has been explained, might be slightly confusing in the sense that there is talk about deference. The question might be what the judge would add in making a decision, if he is going to be so deferential. That is to do with the role the judge has in judicial review, versus the role that the judge would have if the judge was having to authorise it themselves.

I have drawn an analogy here, because it goes back to some of the discussion we overheard from the previous session. There are times when this conversation seems as though it is discussing the difference between political accountability and judicial accountability. One has to remember that the authorisation, in this process, is one very small part of an overall operation, the vast bulk of which is not decided by the Home Secretary or a politician, but is decided by police and judges.

For example, Schedule 5 to the Terrorism Act which is the part that controls terrorist investigations, contains a large number of provisions, production orders and search warrants, including producing material from journalists, all of which are decided by a judge. Those can be much more intrusive, in some circumstances, and much more serious than intercepts, but we trust that to the judge. In serious crime operations, we trust search warrants and production orders to a judge, for a judge to make that decision. The judge does that not by deference to a ministerial decision but by having their own role in terms of making that decision for themselves, and it is a system that works very well with serious crime and under Schedule 5 of the Terrorism Act. That is why one can be led down a

cul-de-sac in thinking that we are choosing here between a brand new type of judicial authorisation or judicial role, when previously it had always been the Home Secretary. In reality in terrorist investigations and in serious crime, it is judges and police who are having to make those decisions and who are accountable for those decisions—sometimes life and death decisions.

Q188 **Victoria Atkins:** I should declare that Peter Carter and I were in chambers together. Mr Carter, you have talked about there not being any provision in the Bill that you can identify for the Secretary of State to give reasons. I have to say, listening to that, I thought, "Crikey, this is a lawyer's paradise". Is it not? We heard from Mr Davis earlier. He estimated that there are 2,300 intercept warrants a year that the Home Secretary does, which equates to nine a day, in addition to all their other duties. If the Home Secretary is having to sit down and write out reasons, in the way that you and I understand as lawyers, I fear that would be a real burden, adding bureaucracy in what is a highly dynamic environment. Is it not better to look at the evidence from the security services or whoever is making the application? Look at that and then the judge looks at it again—the same evidence—and makes their decision according to the evidence placed in front of them by the security services.

Peter Carter: I entirely agree. We do not want this to be a lawyers' paradise. It is going to defeat, not assist, the end. If the law is clear, there is less room for lawyers to get involved. You do not want lawyers getting involved to try to disentangle what ought to be a clear and transparent process for those who need to know about it. My only slight difference of opinion with what you suggested is I do wonder whether the Secretary of State needs to be involved at all, other than in those things that involve the security services.

Q189 **Suella Fernandes:** I have a question; I think Peter and Martin dealt with judicial review. We have heard evidence from Lord Judge and Sir Stanley Burnton, who have stated that they think it does strike the right balance, but proportionality involves a balancing exercise—a consideration of the objective and whether the objective is sufficiently important to justify the intrusion, whether the measures are directly related to the objective and ensuring that it goes no further than what is necessary. Do you not think that that encompasses a very clear and balanced assessment of the decision to issue a warrant?

Peter Carter: I do and those words are perfect, provided they are left alone.

Martin Chamberlain: I have to say that I am not quite so sanguine that the word "proportionality" necessarily connotes a high-intensity review. Within the case law on proportionality, under the Human Rights Act for example, there is still a very broad spectrum of intensity of review and, sometimes, even though the court is looking at proportionality, it gives the decision-maker considerable latitude. In other contexts, it gives the decision-maker rather less latitude.

The problem with simply saying that the standard to be applied is judicial review is that we do not know what arguments the Government will make to the judicial commissioners, and it is quite possible that the Government will say that this is the context, balancing the needs of national security against the intrusion into privacy, where you have to accord considerable latitude and discretion to the elected Minister, and where the judge really should not interfere, unless the Minister has obviously struck the wrong balance.

Suella Fernandes: Just by way of follow-up, would you confirm for the record that, in the process of judicial review, a judge would have access to the same information that was before the Minister throughout the original decision-making process? Is that your understanding of judicial review?

Peter Carter: Victoria Atkins made the point that this is a dynamic process and I entirely agree it is. Given the reality of the situation, particularly if it is a security service application for a warrant, it may well be that, by the time it gets to the reviewing judicial commissioner, which may be 15 minutes or half an hour after the Secretary of State has made a decision, further information is available. The judicial commissioner must take account of all the information that is then available, just in case there has been a shift—either augmented information or something that turns out to need correcting.

Q190 Lord Butler of Brockwell: When Mr Carter read out Section 169(5), saying, "In exercising functions under this Act, a Judicial Commissioner must not act in a way which is contrary to the public interest or prejudicial to—(a) national security, (b) the prevention or detection of serious crime, or (c) the economic well-being of the United Kingdom", I thought to myself, "Crumbs, that really is going to shackle the judge". It is certainly putting pressure on him to approve the warrant, but then I looked down and Section 7 says that that subsection does not apply "in relation to the functions of a Judicial Commissioner of—(a) deciding whether to approve the issue, modification or renewal of a warrant or authorisation". Perhaps you did not intend to mean that it was going to shackle the commissioner.

Peter Carter: No, I do not think it is. What I was concerned about was any suggestion, as perhaps had been made by one of the previous witnesses, that judges were going to be bowled over by a suggestion that this is for national security and, therefore, you must not intervene. The point is that the fact it is there will not prevent the judges from having a rigorous and robust appraisal of the information that is before them, before they make an authorisation or not.

Lord Butler of Brockwell: You are saying that this does not shackle the judge. It will enable the judge to reach full discretion.

Peter Carter: I think so. I hope that the reference to "contrary to the public interest", in any circumstances, would not be something that a judge would find difficult to understand.

Matthew Ryder: I was just going to say, in relation to the point you are making and the point made by Ms Fernandes, it is important to bear in mind that a judge in this position may have access to material, but a judge is not making his own assessment of the facts in judicial review. In the situation where a judge is assessing a search warrant or a production order in relation to something very sensitive, like Schedule 1 to PACE, which could be obtaining material from a journalist, or Schedule 5 to the Terrorism Act, which could be very sensitive and very serious, a judge has the evidence but then assesses that evidence. If the judge thinks the evidence is not sufficient, he could call for more or could look at it.

In a judicial review situation, the judge is essentially bound by decisions and assessments of facts that have been made by the Secretary of State and is applying judicial review principles—which, as Martin rightly says, can be on a range of scrutiny—to that assessment that has already been made of the facts.

The final point to bear in mind is that, normally in judicial review, there is an element of an adversarial process. In other words, the judge is assessing it with somebody making representations in relation to the other side. There will be no adversarial process built into this, the way it stands at the moment. You will have a judicial review, but no one putting forward the argument to the judge in a different situation. Now, that is not unheard of; you have that in other situations, but not in relation to a judicial review situation. That is why it is so important, in this sort of situation, for the judge to be able to be hands-on to potentially look at the facts and evidence in front of the judge, for themselves, and make that decision not shackled by any previous assessment that has been made by the Secretary of State.

Suella Fernandes: Do you not think that that will have a negative effect on timeliness and the speed of decisions, in urgent situations when there are real risks, in terms of the quality of decision-making?

Matthew Ryder: It should not do at all. The reason is that it does not have any problem with timeliness in relation to Schedule 1 of PACE. Those can be extremely urgent applications for very sensitive material in the most intense operations. It does not have any problems in relation to Schedule 5 of the Terrorism Act. I could not imagine a more serious situation, where a judge is having to decide on production orders or search orders in relation to terrorism investigations, under Section 39 of the Terrorism Act 2000, which are then being dealt under Schedule 5 of the Act.

Q191 Lord Strasburger: Not only am I not a politician, I am not a lawyer and I have been struggling through the fog of arguments in this area, since this Committee started to sit. It is only just now that I am beginning to see some light at the end of the tunnel. Are you collectively saying that the solution to this whole problem is to strike out the phrase that includes the words "judicial review"?

Peter Carter: Are you asking four lawyers to agree?

Lord Strasburger: I will settle for your individual opinion.

Peter Carter: My opinion is yes.

Martin Chamberlain: Mine is, too. It would be much clearer if you said to the judicial commissioners what standard you are expecting them to apply. You could do that in various ways. One way would be to get rid of the words "judicial review", which imply this shifting spectrum, without telling you where on the spectrum you are.

Matthew Ryder: I would still be inclined towards judicial authorisation by a judge, rather than judicial approval. I certainly think in relation to police cases that "judicial authorisation" would be appropriate. In national security cases, you can have a different discussion, but my preference would be "judicial authorisation", rather than "judicial approval".

Graham Smith: I am a mere IT and internet lawyer. I would not begin to venture an opinion on this.

Lord Strasburger: May I then ask the opposite question? What do those words add to the Bill? What benefit do they bring, if any?

Martin Chamberlain: The suspicion or the worry is that it may be argued by the Government, once this Bill becomes an Act, that what they add is a clear signal or flag to the judicial commissioner that, when you are examining warrants issued by an elected official, you should back off and not question those warrants, unless the decision to issue them was irrational or something close to irrational. Probably "irrational" is the wrong word, because clearly proportionality comes into it but, at the far end of the spectrum, that is the worry. It would be very interesting to hear what the Government say in response to that. If they were to say, very clearly, "That is not what we intend. We intend it to be intensive review", and if they were to say it in a way that could then be subsequently relied on in legal proceedings, that would be very interesting.

Q192 Dr Murrison: We have moved quite a long way towards the double lock. The double lock was a point of some controversy, but has now been accepted by the Government. It is worth just recording that. What you are saying is that you would be happy with the deletion of Clause 19(2), which we heard, for example from Liberty the other day, would materially improve the Bill and the scrutiny available.

May I press you on this five-day period, during which the judicial commissioner would take a view, albeit in the Bill at the moment a rather limited view, on the authorisation that the Secretary of State has given? Do you feel that five days is reasonable, since we have heard from others that it is a very long time for a judge to form a view, particularly since he is likely to be presented with the same sort of material that the Home Secretary deals with, sometimes with a very short timeframe? Indeed, that of course is used as a justification for the Home Secretary dealing with this in what have been characterised as emergency situations, not a judge. May I start? This is something that the Bar Council is particularly concerned about. We can see no justification for that five-day gap. The Secretary of State is a single person. Numerous judicial commissioners can be appointed and, no doubt, will be appointed under the Bill. High Court judges are used to dealing with applications of the utmost urgency.

When there is a need for an urgent application, for example a place of safety order or to prevent somebody being deported from the United Kingdom, I am afraid judges used to be wakened at any time of the day or night and can deal with that matter, as a matter of urgency. There is no reason why a judicial commissioner cannot deal with it as a matter of urgency. For example, a judicial commissioner might be in a position, as the Home Secretary probably might not, under the Bill, to say, "Yes, I authorise this warrant and I want you to come back in 24 hours and I will review my decision and how far it had got". There is provision for that in the Bill, but I can see that practice would develop whereby a judge would make an authorisation that was interim and conditional. I cannot see any reason why five days for a warrant that is potentially unlawful can be justified.

The Chairman: Can you suggest a time?

Peter Carter: I do not think there is any justification for any time, any delay. The delay, if anything, is going to be with the Home Secretary, not with the judicial commissioner.

The Chairman: The issue is one of urgency here, is it not? These are only urgent warrants. We are not talking about the 2,500 to 3,000 warrants that have to go through the various Secretaries of State. We talk about a much smaller number. Would that make a difference in terms of, I do not know, a day afterwards?

Peter Carter: The difficulty about that is that, if it is urgent, you should not prescribe a time limit because, if it is urgent, it must be done immediately.

The Chairman: Indeed, but the issue is if there is a joint authorisation, which there is on a normal warrant, but an urgent one, because of its very nature and what might be happening, the Secretary of State obviously has to authorise. The Bill says you can have up to five days for a judicial commissioner to review that, but you do not think there is any need for any sort of time limit. It depends on the availability of the judicial commissioner, presumably.

Peter Carter: There will be a judicial commissioner available at all times. There should be. It may well be that, if it really is urgent, the Home Secretary or the Secretary of State should be, as it were, a bystanding participant and it should be a single, consolidated process.

Matt Warman: How does that work?

Paul Hudson: The principal decision-maker and authoriser would be the judge. It would be subject to the Home Secretary saying, yes, he or she confirms that it is necessary, so you do it the other way round, in a sense.

The Chairman: To put in my own experience, from when I used to authorise warrants as a Secretary of State—very urgent ones, virtually in the middle of the night or something—you are not going to sit there and have to phone up a judge immediately, when something might have to be decided in minutes, surely.

Peter Carter: That is why I am suggesting that the only reason for having the Home Secretary's decision is this double lock process, is it not? The presumption is that the Home Secretary is a politician who is attuned to security needs and would be the first port of call but, in urgent cases, there is no need for that. The first and only port of call is the judge. If the Home Secretary, having been informed of the information says, "Actually, I disagree", which is highly unlikely, the Home Secretary would then have the power to revoke it.

The Chairman: Why are you suggesting that it should go to the judge before the Home Secretary in an urgent case?

Peter Carter: It is because you then have the consistency of every such warrant having judicial approval.

The Chairman: I understand.

Q193 Bishop of Chester: Is it possible to try to situate this whole discussion between the European culture, which has experienced totalitarian Governments and has a suspicion of government with the history of totalitarian interference, and North America, where there has always been that freedom of the individual and a small state. We are somewhere in between. There is a danger of these wide-ranging powers, which you have identified, being accepted

too easily, hence the need for some sort of robust double lock and a strong culture of judicial independence in the judicial element, I suggest. One of the questions we have raised is if the judges should be appointed by the Prime Minister or by the Judicial Appointments Commission. Should they be appointed for a single term of office, rather than have to submit to reappointment? There are these sorts of questions. Are there other ways of strengthening that culture of independence that you all want to see in the judicial involvement?

Peter Carter: Given the gravity of the kind of situation that is envisaged in this Bill, I would have thought that the appropriate candidates for judicial commissioners are likely to be High Court judges. It may be that it is because we have all gone native in the profession that we see no reason to doubt the integrity and the robustness of people who satisfy the criteria of appointment to the High Court bench. I do think, though, that there is a potential problem of perception, if not reality, if appointment to the judicial commission is by the Prime Minister, rather than by the Judicial Appointments Commission, with consultation with the Lord Chief Justice. That would be more appropriate, rather than it looking like a political appointment.

Bishop of Chester: Would you review after three years, as is proposed, or is it better and more of a culture of independence to appoint for a single longer term?

Peter Carter: I am not particularly bothered. Others may take a different view about that but, if you are appointing somebody of the category I have suggested, either they will be sitting senior judges, in which case after three years they may go back to their normal judicial appointment; or they may have retired, in which case three years would probably be sufficient for them to feel that they have done their job and would quite like to go and do something else. Potentially, it will be quite an onerous job. For somebody in this position, I do not see that there is a problem about the perception of independence from it being a three-year term, in the same way as, for example, for the appointment of the Director of Public Prosecutions, the term is sometimes three years and sometimes five years. Nobody, so far as I am aware, has made any suggestion of lack of independence as a result of a three-year, as opposed to a five-year, term of appointment.

Matthew Ryder: Three years is a short tenure for a judge and it might be that the Judicial Appointments Commission would be well placed to express a view about that sort of time in relation to judicial independence, because they have done some significant thinking on how long tenures should be for judges, to ensure that judges do not feel vulnerable when they next come up for review.

Bishop of Chester: When they appeared before us, the impression given by the judges was that they generally sided with the application. David Pannick's article referred to that benefit of the doubt or margin of discretion or whatever it was he said. I cannot remember the term you used there. One can see that a certain culture of it being normal to go along with the Executive could develop without quite being noticed. I simply put this up for you to demolish. Others who have sat in those seats would certainly have those anxieties.

Peter Carter: All you have to do perhaps is look at the history of the current Investigatory Powers Tribunal and the independence that has shown in standing up against the Government's attempts to keep secret the unlawfulness of some of the conduct, and the tribunal's insistence on making public as much of its judgments as it possibly can.

Martin Chamberlain: I would agree with that. I do not think you need to worry that the people who are appointed to these rules will slip into a culture of doing what the Executive want. What you need to worry about is that judges, in performing their role, will do what they think Parliament has told them to do. If they think Parliament has told them, by use of words like "judicial review", to accord considerable latitude to a constitutionally accountable Minister, then that is what they will do. That is not because they are unable to stand up to the Executive; it is because they are honestly interpreting what you have said to them. If you do not want them to apply considerable latitude, you need to make clear that they are not to do so. If you make that clear, they will do what you say.

Q194 **Victoria Atkins:** Lord Chairman, I am very conscious that I am about to venture into a subject in which you are an expert and I am not, but it is a simple question. Have you taken into account the political sensitivities of Northern Ireland and the way the judiciary is viewed by some, in different parts of that part of the country, when assessing the argument that judges should always come first?

Peter Carter: No.

Martin Chamberlain: I have not either, but I would have thought that, if and to the extent that there are elements of the community in Northern Ireland who have less confidence in the judiciary than perhaps people would have in England and Wales, or Scotland, then one would have thought that those same elements would have a similar lack of confidence or even a greater lack of confidence in members of the Executive.

Dr Murrison: I have a very quick supplementary to that. Do you think then that that is another argument in favour of the Judicial Appointments Commission appointing commissioners, rather than the Prime Minister? If the Prime Minister appoints the judicial commissioners in relation to Northern Ireland, one would also have to involve the First and Deputy First Ministers.

Peter Carter: I first heard that argument raised at a meeting in Portcullis House on the eighth of this month, and it struck me then that I wished I had thought about it before. It seems a very good suggestion.

Q195 **Suella Fernandes:** The Home Secretary will have the power to amend the functions of the judicial commissioners. How do you envisage that power being exercised and what kind of modification might be envisaged?

Matthew Ryder: I do not know is my answer.

Martin Chamberlain: I would say the same. It is very difficult to envisage how it might be exercised. In principle, it could be exercised to add to the functions or to take away from the functions. One potentially worrying use of the power would be if it could be used to alter the test that a judicial commissioner has to apply when considering or reviewing the issue of a warrant. I do not know whether it is intended to use the power or that the power might be used in that way, and it would be an interesting question to get the Government's view on.

Peter Carter: Can I make a suggestion? It seems to me that the power to modify the commissioner's role should be confined to those roles that are not central to the authorisation of warrants and the continuation or renewal of warrants.

The Committee suspended for a Division in the House.

Peter Carter: I am very grateful for that, because it has allowed me to find my place in the notes. The question was about the Home Secretary's power to modify the role of the judicial commissioner, which appears in Clause 177. In the clause as it stands, there are no constraints as to which role or part of the role the Home Secretary can amend. This means that, if you decide to remove the expression "judicial review", the Home Secretary could, by his or her power of amendment, depending on who it was at the time, put it straight back in again, which may not be entirely satisfactory.

This provision, Clause 177, appears in part 8 of the Bill. There are various provisions there that explain or provide particular functions for commissioners, including that the investigatory powers commissioner in Clause 169 must keep under review the exercise by public authorities of statutory functions, and so on. I can understand why that kind of role or function is suitable for amendment, as circumstances and the law change. What I would suggest is that Clause 177 should be amended by adding the words, in subsection (3), "This clause does not apply to any function of the judicial commissioner under parts 1 to 7 of this Act".

Q196 **Victoria Atkins:** I am conscious of the time. Mr Carter, you have written a very helpful paper, on behalf of the Bar Council, regarding legal professional privilege or LPP. Can you help us with any concerns about LPP and investigatory powers and, if there are concerns, how they can be addressed? How would you recommend they be addressed?

Peter Carter: We have concerns, because there is nothing in this Bill that protects legal professional privilege. Legal professional privilege is the privilege of a client to have private communication with a lawyer, to obtain legal advice or for advice and assistance in the course of litigation, whether active or potential. Communications between a lawyer and a client are not all protected by legal professional privilege, and we are not suggesting that all communications between a lawyer and a client should be protected or immune from investigatory powers. For example, the Proceeds of Crime Act makes it quite clear that communications between a lawyer and a client covered by legal professional privilege are immune, but a client asking a lawyer for advice on where the best place is to stash his stolen loot is not. If there was information that led the police or the security services to believe that that conversation was about to take place, then they would be fully entitled, and I would applaud them, for putting in place some of the provisions of this Bill to get evidence that that was taking place.

The difficulty is that, if legal professional privilege, properly so-called, is not recognised as a privilege that needs to be protected, it strikes at the heart of our judicial system, not just the criminal system, but the judicial system. It is the integrity of the judicial system that is one of the guarantors of our state as a democracy.

Imagine the situation if a client in a commercial action were to say to me or one of my colleagues, "I am about to engage on a contract and I need your advice as to the international effects of this. It is with a Russian company. It is very sensitive because I have competitors in other states. Can you assure me that all our communications will be confidential?". Under this Bill, my answer would be, "No, I cannot", because I simply do not know.

The difficulty is that the wording used in Clauses 5 and 65 says that, where a warrant authorises any of the investigatory powers under this Bill, then any action taken in accordance with that warrant is lawful for all purposes. If the warrant authorises the interception or the gathering of data information concerning communications between me and the client, it would be lawful, even though under international law, European law and our historic law, such communications have been immune, as a matter of public interest. The fact that these rights are ancient is neither here nor there; what matters is that they are current and they are important. They are important for the confidence of citizens in the administration of justice.

Interestingly, when David Anderson produced his report, *A Question of Trust*, in a fairly short passage, he described why legal professional privilege is important. He said, if it is apparent that there is no guarantee that legal professional privilege is protected, it will have what he called "a chilling effect" on the relationship between client and lawyers, and their confidence in the entirety of our judicial system.

The Government fight fiercely for its own legal professional privilege, particularly for example when it is engaged in international arbitration. The Belhaj judgment in the Investigatory Powers Tribunal said this, "There was no dispute between the parties", that is between the state and Belhaj, "as to the importance of protecting and preserving the concept of legal and professional privilege". Why, therefore, is that recognised importance not reflected in the Bill? It is in various other statutes, including in the Terrorism Act 2000 and in the Proceeds of Crime Act, as I have already identified, and in the Police and Criminal Evidence Act.

The problem is that there was one clause, in the Regulation of Investigatory Powers Act, Section 27, that used that expression, "lawful for all purposes". The House of Lords by a majority decided that that empowered a warrant to enable the investigating services, police and intelligence services to intercept communications covered by legal professional privilege between a lawyer and a client. In fact, what was uncovered out of that was of precious little significance, but it was a chilling effect. It has had a chilling effect. Those of us who practise sometimes in criminal law realise that what you require is to build up the confidence of a client in order to give robust advice, sometimes advice that they do not want to hear, but they need to hear. If they cannot be confident that the communication is confidential and secret, they will simply say nothing. That does not help anybody or anything.

Why is it not there? It is said by the Home Office that it is all right; it will be in codes of practice. Interestingly, Schedule 6 contains the only reference to something akin to legal professional privilege, and it is in paragraph 4 of Schedule 6. It says, "A code of practice about the obtaining or holding of communications data by virtue of part 3", so it is confined to the powers exercised under part 3, not under any other part, "must include … (b)

provision about particular considerations applicable to any data which relates to a member of a profession which routinely holds legally privileged information", which I assume means lawyers.

There are two things that follow from that. The first is that it recognises, as is evident from the proceedings in the Investigatory Powers Tribunal, that the security services have access to sufficient information to be able to filter those communications that are communications with lawyers, so they know which communications are likely to trigger access to data or communications, which are or the subject matter of which is covered by legal professional privilege. They can do that.

Why is it that the codes of practice under paragraph 4 of Schedule 6 are confined to this particular area under Part 3? The codes of practice or the draft new codes under the Regulation of Investigatory Powers Act also have a provision about legal professional privilege, which does not guarantee the immunity of legally privileged material from access by and disclosure to the agents of the state. It simply says it is a serious consideration, before authorisation is given, not only when it turns out that legally privileged material has been accessed inadvertently, as part of a more general and legitimate operation, but even when it has been specifically targeted.

Whether that will survive a challenge in the European Court of Justice or in Strasbourg, I have my doubts. I am not certain about it, but I have my doubts and I have my doubts because, in international and in regional human rights law, one of the critical basic rights is the right to independent advice or advice from an independent lawyer. Advice from an independent lawyer is going to be worthless if the client and the lawyer believe that everything said is going to be heard by or accessed by the state.

The state, in the cases that are dealt with in the Investigatory Powers Bill, will in most cases, the chances are, face some kind of litigation involving not necessarily the person whose communications are accessed, but somebody else. Eventually, the chances are, the litigation, whether it be criminal or civil, will indeed be between the person whose communications are accessed and the state. The state would not want to be at a disadvantage if another state in international arbitration had access to all its advice. There have been various expressions about the importance of this right over the centuries but, as I say, what matters is its significance now as a right in a democratic society, which is regarded as a guarantee of a democratic principle and a guarantee that citizens are not at a disadvantage in their dealings with the state.

The Chairman: I shall have to curtail things in a second. I am just asking whether your colleagues agree with what you have said on this or have any additional points.

Matthew Ryder: I do not have anything to add.

Martin Chamberlain: Neither do I.

The Chairman: There is no dissention, which is very good. I am going to close the session now. We have, however, a number of questions we would like to put, if that is okay, to all four of you, in writing. I am conscious of your time, but I am also conscious of the fact that I do not particularly want these questions or the answers to them to be missed. If that is okay

with you, we will write to you. We are very grateful. It has been a fascinating sessions and a very important session for this Committee. Thank you so much for coming.

Bob Satchwell, Society of Editors (QQ 137-144)

Evidence heard in public Questions 137-144

Oral Evidence

Taken before the Joint Committee

on Monday 14 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Stuart C McDonald MP, Matt Warman MP, Baroness Browning , Lord Butler of Brockwell, Bishop of Chester, Lord Henley, and Lord Strasburger.

Witness: **Bob Satchwell**, Society of Editors, gave evidence.

Q137 **The Chairman**: A very warm welcome to our witnesses today. I know there was not very long notice for everyone, but thanks to all four of you for coming along to give your thoughts on what is regarded as probably one of the most significant Bills of this Session. As in previous sessions and in any similar parliamentary committee, we will ask you a number of questions, which I hope will stimulate your brain cells. We will have a dialogue with you in this particular session about the importance of privilege to the legal and journalistic professions.

I am going to start by asking a question about the legal professional privilege. How do you think the draft Bill addresses the concerns of the legal profession about privilege and the investigatory powers in England, Wales and, of course, Scotland? Does it create any new issues?

Colin Passmore: It falls to me, as the lawyer among the four of us, to see if I can address that. My name is Colin Passmore. I have been a solicitor for 31 years now and I can modestly claim to be an expert on privilege because I write the leading textbook. I am sad enough to know the thousands and thousands of cases on privilege and the hundreds and hundreds of statutes that deal with privilege. What is unique about RIPA and this Bill is that, on the face of it, they do absolutely nothing to address the concerns that the legal profession has about privilege and the way in which surveillance techniques in all their glory can be used to infringe the privilege.

Privilege, as I am sure you know, is possibly the highest right known to the law. It is over 500 years old. It is jealously guarded, not only by the legal profession but by the courts, with the result that there are usually hundreds of cases in London alone every year in which challenges to privilege are upheld. In addition, in every single statute that confers investigatory powers of any sort, whether we are talking about the police, the SFO, the Revenue, even local weights and measures departments, there is always a provision that actively protects privilege, so nobody—the police, the Revenue—has the ability to force any client to divulge their privilege. The same thing happens in statutory instruments. This draft legislation and its predecessor are unique in that there is nothing in them that protects privilege.

When this issue came before the House of Lords in the McE case from Ireland some years ago, it is fair to say that the legal profession was extremely surprised that Section 27 had the ability to enable the security services, the police and others at least to listen in to privileged communications in certain circumstances. Even the House of Lords in that case indicated a great reluctance to interpret Section 27 as giving the ability to listen in on privilege, but the House of Lords proceeded quite clearly on the basis that this happens very, very rarely. The House of Lords was at pains to say that if it happens on a regular basis there will be a chilling effect on privilege. The chilling effect is really important, because it inhibits the frankness of clients, whose right it is, with which they speak to lawyers. If that chilling effect is in play, it could undermine the right to a fair trial under Article 6, infringing on privacy rights under Article 8, and undermining the administration of justice.

We know now, from cases like the Belhaj case and other cases that have come to light in the last year, that whereas we thought this interference with privilege was very, very rare, it is happening far too often and on a routine basis. In my view and the Law Society's view, unless this legislation is amended so as to deal with privilege on its face, then privilege, this very old and supremely unique right—there is nothing else like it in any form of communication—begins to become seriously undermined.

The Chairman: Mr Musson, do you want to add anything to that?

Tim Musson: Not a great deal, Lord Chairman. My background is not legal professional privilege in the same way as Mr Passmore's. I am here to represent the Law Society of Scotland. It appears that legal professional privilege in Scotland is very similar to that in England and Wales. The differences are absolutely minimal, although it has arisen in a slightly different way. There are the two sides to the privilege: England started on one side, Scotland started on the other side, and they have come together. Certainly the Law Society of Scotland is very concerned about the erosion of legal professional privilege that appears to be quite possible with this Bill. They have great concerns about it, which do not differ in any way from what Mr Passmore was saying.

The Chairman: Picking up on where Mr Passmore finished, and now that you have added to his comments, it is very appropriate for our only Scottish member to come in on the issue of any possible amendments.

Q138 Stuart C McDonald: Mr Passmore, you suggested that this Bill will need some amendments before you are happy with its approach to privilege. Can you give us any more indication of what sort of amendments you think would be required?

Colin Passmore: There is a serious question as to whether there should be a prohibition on interference with privilege at all. Why is this interference necessary? I respectfully suggest that there are not many cases where lawyers, be they solicitors, barristers, advocates, have been found guilty of abusing the privilege. If a solicitor or a client in their relationship with a solicitor abuses the privilege, the privilege falls away. There is something known as the crime-fraud exception or the iniquity exception.

You do not need these seemingly open powers to listen in to solicitor-client conversations unless you have some evidence that there is something wrong going on. There is very little evidence that solicitors or lawyers abuse the privilege, and therefore the power to listen

in, to intercept or to hack is simply, in my view, unnecessary. I would be a strong advocate, and the Law Society is a strong advocate, joined by Scotland and indeed other jurisdictions, for having the type of privilege preservation clause that you find in all other statutes, including those that deal with police powers, revenue powers and so forth. I respectfully suggest that there needs to be a provision in here that makes it clear privilege is out of court.

Stuart C McDonald: Are you frustrated, then, that sometimes we hear from the Home Office that they are scared of putting some kind of prohibition on intercepting legal privilege because of the risk of abuse? You are saying to us in effect that that abuse means that the privilege no longer applies.

Colin Passmore: That is my view. I know many lawyers who understand the importance of privilege and its unique status as a means of privacy in communications with clients. Many lawyers whom I know take the obligations that arise from having the benefits of privilege very seriously. I can think of a handful of cases in which privilege has been abused; I am aware of one, which came to my attention this morning, that has just gone up to the European Court of Human Rights. It simply, in my view, does not happen that lawyers abuse the privilege.

Stuart C McDonald: Mr Musson, do you also seek that prohibition in the Bill?

Tim Musson: Ideally, yes, I would seek that. If it cannot be taken as far as that, there become issues about who is competent to permit interception of these communications. It would need to be someone who understands legal professional privilege, and the sort of person involved in this authorisation might not have that knowledge or understanding.

Q139 Lord Butler of Brockwell: Mr Passmore is making the case for prohibition on the grounds that privilege falls away if a lawyer is engaged in criminal activity. In those cases, you would say that there must be evidence that that is happening, but then you are putting too much power in the hands of the authorities, are you not? They say, "We have evidence"—let us say this is the Home Secretary—"and, therefore, please may we have a warrant to listen to this lawyer because we think privilege has fallen away?". Would you not rather have a stronger safeguard than that, a formal procedure that certifies that that is the case, rather than just the judgment of the Executive?

Colin Passmore: That is a good point. I do not make the case just on the basis of the iniquities exception. I make the case primarily on the sheer importance to the administration of justice of the privilege itself. I am very concerned that this Bill has the ability to undermine privilege more generally. With regard to your second point, in the way this iniquity exception works with, for example, the police, the SFO or the Revenue authorities, when they seek a warrant to go into a solicitor's office, they have to satisfy the judge in the Crown Court that there is a really good case for being able to go into the solicitor's office, knock on the door and start to take papers away.

Forgive me, I am going slightly off your point but I will come back to it. If privileged materials are identified, whether or not the exception applies there is always an independent lawyer in attendance who will do the physical bagging up of the documents or the computer disks, and he or she will later go away to determine whether they are privileged. There should be

a check, of course, but a judge is more than capable of looking at the evidence as to whether or not the iniquity exception is likely to apply. Judges are very good at this.

Lord Butler of Brockwell: Would that not be covered by the new procedure under this Act: that if the Home Secretary is to grant a warrant, it has to be endorsed by a judge?

Colin Passmore: Yes, as long as the reference to the judicial review standard is removed—first, because that introduces an element of ambiguity: what is the judicial review standard? I know that eminent lawyers such as David Pannick have written to say that it is fine; I know many others who disagree with that. But I am not even sure why we need that. If the communication that the authorities wish to intercept is subject to the iniquity exception, that of itself should be enough; we do not need a judicial review standard. Does the exception apply prima facie or does it not? If a judge is not happy that the exception applies, the warrant or the ability to intercept simply should not be granted.

Lord Butler of Brockwell: That, if I may say so, raises a slightly different point. I am not trying to put words in your mouth, but I think you are saying that if the judicial review test was removed, you would be content with a procedure whereby the Home Secretary can grant a warrant, provided it is endorsed by a judge, if there is a really good case?

Colin Passmore: Coupled with an express recognition in the draft Bill, in the statute, that privileged material is not available, that would be great. I would be happy with that and I think the Law Society would be.

Bishop of Chester: The closest parallel might be a confessional and a priest. It is humorous on one level but serious on another. It is on a much lower level than legal privilege, but what qualification there is to an iniquity exception is a matter of contemporary discussion. It may apply only to the Church of England, but we have other religious groups in our country now. I would have thought that if we are going to put something in the Bill, in principle we should, I suggest, at least look at whether that is a parallel set of circumstances, because putting a bugging device in a confessional situation raises the same sort of issues in a different context.

Colin Passmore: It does. I am sorry to disappoint you, but the law addresses privilege as a higher right capable of greater protection than the confessional box. It is easier to get disclosure of your conversations with a confessor than it is my conversations with my client. I am not saying it is very easy; it is very difficult, but I am afraid privilege is on a slightly higher plane so far as the English and Scottish courts are concerned.

Victoria Atkins: To clarify, on the point of the iniquity exception, your evidence is that you wish protection to be put into the Bill that reflects the law as it stands currently across all other statutes, so if a solicitor is trying to commit a crime with their client, that information will not be protected by privilege?

Colin Passmore: Absolutely right. It cannot be protected.

Victoria Atkins: You gave the example of search warrants. Interception warrants are a much rarer event even than the pretty rare event of HMRC or whoever going into a lawyer's office. The safeguards are there, surely, for interception warrants, given how rarely, particularly in secure environments and so on, these are used.

Colin Passmore: The occasions that we know of when cases in which the police have sought interception warrants have come before the courts are relatively rare, and you have to go through the Crown Court judge warrant procedure and satisfy the judge that the iniquity exception is likely to apply. I am a long way from being an expert on interception and the security services, but I have been slightly horrified this year at the number of cases, starting with Belhaj and others, that have come before the IPT in which these issues are raised. I am not myself convinced, although I am not an expert—far from it—that these cases are such a rarity. I would therefore far rather the security services et al had in the Bill the clear recognition of just how important privilege is, plus the mechanism of going via the judge.

Q140 Suella Fernandes: Thank you for your evidence today. Do you agree that someone who belongs to one of these professions that we are talking about, maybe the legal profession or the journalistic profession, may also, albeit in rare cases, pose a threat to national security, and in those cases it is important that the agencies have a power to intercept their communications?

Colin Passmore: I find it difficult to think of a case that would be any more than a rarity. I am aware of one case in Northern Ireland, which is the case I alluded to earlier that has just gone up to the European Court of Human Rights, where a solicitor conspired with his alleged terrorist client to bump off a witness. That is incredibly rare. It is so rare it is shocking. I am not aware of any cases where that is likely to happen. I am not suggesting for a moment that every single member of the legal profession in the UK is beyond reproach—of course not—but I find that a difficult concept to get my head around.

Suella Fernandes: Do you appreciate that the agencies have given evidence that they would never specifically seek to acquire privileged material except when they apply for a specific warrant?

Colin Passmore: I would give you the lawyer's answer to that, inevitably, which is that if that is the case, they cannot have a problem with the Bill recognising the importance of privilege. In other words, if they recognise that they do not want privilege, let us put it in here and make sure it is beyond doubt. Then, if there is a circumstance in which the iniquity exception applies, go to your judge for your warrant. If your evidence is good enough, fine, you are up and running.

Suella Fernandes: Lastly, it is always subject to the test of being necessary and proportionate and that the intelligence cannot be obtained in a less intrusive way.

Colin Passmore: That I disagree with. The courts and some very famous names in the judiciary, such as Lord Denning—I am showing my age—and others since have recognised that the consequence of a claim to privilege is that the court, the Revenue and the police are deprived of what they regard as potentially relevant evidence. It is a consequence that we have to face with an assertion of privilege.

Bob Satchwell: I think your question was: could it be possible? It would be foolhardy of me to say that it was impossible, but it would be astonishing. There are so many examples of the way journalists understand and very carefully apply restrictions upon themselves in relation to national security issues through the DSMA committee, through what were

wrongly called D-notices, and things like that. We work like that all the time. I have never known of a journalist who would ever have put someone's life or national security at risk inadvertently. What we are concerned about is precisely the point that there need to be very clear procedures and rules if someone is seeking to invade the journalist's activities and his sources. More recently, and perhaps we will come on to this, the evidence has been that some organisations rode roughshod over something that we all thought was accepted.

Q141 **Victoria Atkins**: What is the legal status of the codes of practice under RIPA?

Colin Passmore: Vague. They are the worst option for dealing with this issue, in our view. We have a problem here at the moment in that the codes of practice that will be developed pursuant to this are so far unwritten, although I imagine they are going to reflect a lot of what is in the present codes. A code of practice is what it says on the tin: it is a code. We have seen from recent cases where the security services have breached the code that there is not really a sanction. There may be some disciplinary sanctions, but we have seen that the remedies available in the ITP are pretty low-key compared with what one might expect to get, for example, in the High Court, where there might be a claim arising out of a breach.

They are clearly not of the status of legislation. In the absence of something in the Bill, something in the Act to be, that makes the status of privilege clear, the code of practice is always going to suffer, in our view, from this weakness that cannot be cured, no matter what you put in it. It is a code. It is slightly better than the *Highway Code*.

Victoria Atkins: Should we not separate between security services and law enforcement on this issue? As you know, under the codes of practice for the Police and Criminal Evidence Act, there are very real ramifications for the prosecution if the police fail to follow the code. The case may be dropped.

Colin Passmore: I totally agree, but the big difference is that the Police and Criminal Evidence Act, or the Criminal Justice Act for the SFO, makes it clear that privilege is untouchable. You have this primary legislative direction that we do not have here, nor with RIPA. Therefore, the codes of practice are bound to suffer from that. The codes of practice currently have all lovely things about privilege, but they are effectively unenforceable. You have to trust the operatives in the security services to make sure that they will obey them and that they will adhere to them. Personally, I do not think that is good enough when we are dealing with privilege, which as I keep saying is this extraordinary right, which should be protected in the primarily legislation.

Victoria Atkins: What do you expect to be contained in the codes of practice issued under this Bill?

Colin Passmore: That depends what is in the Bill. I would like to see in the Bill: a recognition that privilege is untouchable and that therefore there should be a fair amount of guidance to the security services and others on what privilege is, why it is so important and what the consequences are of coming across it: a very clear statement, if I may suggest, that there is no basis whatsoever for targeting it deliberately; a very clear explanation of what the iniquity exception should be; and a very, very clear statement of the dangers of playing fast and loose with privilege. You may ultimately cause a trial to be stayed because you have interfered with a defendant's right to a fair trial; you have interfered with his or her

privilege. There would need to be a lot, in my view, in the code of practice. I do believe that it has to emanate from the primary direction in the Bill as to the importance of privilege.

Victoria Atkins: I have a final question on that. The commissioners will play a very important role under the draft Bill as it stands at the moment. Is it not sufficient to trust them with bearing that very much in mind when they are looking at individual applications, and in due course reviewing how the legislation is being applied generally?

Colin Passmore: The intent of the legislation is that there would be a senior judicial officer, at least at Court of Appeal level or above, so really senior, experienced lawyers. Provided they also have the direction in here that privilege is untouchable unless the iniquity exception is in play, I would be happy with that.

The Chairman: Thank you very much. We turn now to journalistic provision and privilege, touched on Clause 61 of the Bill.

Q142 Suella Fernandes: Clause 61 requires that a judicial commissioner approves the issuing of any warrants for obtention by agencies. What is your view of that safeguard in protecting the media's rights?

Bob Satchwell: Our simple view is that it does not go far enough. Some interim measures have been put in place to do with RIPA and so on, but the difficulty is that RIPA was used—I have always argued that it was misused, actually—in certain cases, some of which became very full of headlines and so on, to get around the good safeguards that are in PACE. A number of examples that learned lawyers have come up with—I am not a lawyer, by the way—show that that happened.

The key point with legislation of this kind is that we know what the basic intention is in these troubled times, but that is why legislation was enacted previously. I remember when RIPA was enacted it was made clear to me by Ministers whom I talked to, and I believe it was the will of Parliament, that RIPA was supposed to be an Act to do with fighting terrorism. We have found that, in fact, it became something completely different.

I start by saying that it is very important that the legislation—with all due respect to those who may have been involved in that legislation originally; no one expected that it would be misused in the way it came to be misused—is very clear what the ground rules are before you even get to the codes of practice. Codes of practice are fine so long as someone follows those codes of practice. It absolutely needs to understand, as most people understand—it is something I have always had in my mind, and I have been 40 years a journalist—the first rule of journalism: that you protect your sources. That is in other parts of legislation. It is understood in Europe. It is understood in most places. Judges will very rarely make a journalist reveal his sources, and so on. That background has been totally misunderstood by the police for example, who have ridden roughshod over those principles. Somehow it has to be there very, very clearly.

Going back to your previous question about the possibility of a journalist being involved in something that was against the national interest, they have to come up with evidence, not a fishing expedition; it has to go before a judicial authority. What is more, there has to be

an opportunity for the media organisation to argue and to explain the case, because it is not just a matter of delving into journalist records or into who those sources are.

An inquiry into certain parts of a journalist's activity may inadvertently reveal a source that the police or the security services are not interested in. That is why it is very important that there is an opportunity to know when the police or the security services are asking for that, and an ability to argue that case.

The Chairman: Mr Smith, do you want to comment?

Andy Smith: Yes, just to pick up and elaborate on a couple of things that Bob has said. The NUJ agrees that, while not ideal, the provision under PACE is one that we have been able to work with. We have been able not only to oppose some applications outright but to use the knowledge that we have as journalists to explain the situation that we are in, so that a judge can make a variation of something in front of him, which, as far as I can see, is very difficult under the framework that you have in front of you. A police force may come and ask for hundreds of hours of video tape and end up with 10 or 15 seconds that the judge considers to be pertinent to the application they have made.

To be clear, what we have under PACE, as Bob said, is: prior notification, which we think is absolutely essential; sufficient information about the application, for instance what other means have been attempted to obtain the information, so that we are treated not as a first resort but as a last resort; the importance of a face-to-face hearing, which is not about journalists having their day in court but about being able to demonstrate, particularly to potential sources of information, that the journalist's commitment to protect their sources goes up to defending them in open court and going to bat on their behalf; and a rigorous right to appeal before approval is granted. Under the draft legislation, there is an ability for the force or body making the application to appeal, but there is no right to appeal for any of the persons affected, simply because they are not told.

The only other point I would make initially is on the business of communications data, as opposed to the information contained in the communication itself. Journalists are in a very particular position, in that very often the information gathered has already been published and the most important thing is the fact of the communication. The communications data is at least as important as the content of the communication, quite possibly even more so, given our commitment to protect journalistic sources. It is a very particular situation that journalists are in in that respect.

Suella Fernandes: I have one final question. Special protection requires special responsibility, and in some professions the communications between the professional and their client are very well-regulated, for example the medical profession or the legal profession. There are regulations covering journalists, but they are very different from the regulations that apply to the other professions. Do you agree with that?

Bob Satchwell: Yes. It is quite reasonable. Journalism is not a profession in the sense that the professions are professions. It is not a closed shop in that sense.

The Committee suspended for a Division in the House.

Bob Satchwell: But I hope that we always act professionally, which is somewhat different. In all the codes of practice that journalists have, whether for newspapers and magazines or in broadcasting and so on, there is a simple recognition that the protection of sources is a moral duty, as it is put. That is recognised by the courts, by European authorities and so on.

Andy Smith: The other thing PACE does is concentrate on journalistic material. If a journalist, however they want to label themselves, is doing anything that is outside of that journalistic function, it is not covered. Bob talked about the times when legal privilege falls away, and, in a similar way, material that the police want to access concerning a journalist doing something other than their job would not be covered.

Suella Fernandes: The point I want to make is that there is much less regulation for journalists compared to the other professions, and the definition of a journalist is not as clear cut as it is for members of the legal or medical professions.

Bob Satchwell: That is true, but just because the regulation is not quite as formal does not mean that it is not followed. In some circumstances, the following of journalistic practice, which is accepted across the industry, is stronger because it is not laid down in legislation. The fact that it is peer judgments means that people will adhere to it.

On the question of sources and the release of information, it has been recognised in legislation and it is recognised in the courts that sources and other journalistic material should be delved into only in special circumstances.

Q143 **Matt Warman**: I should declare an interest. I am a member of the NUJ, although, I suppose, a recovering journalist. To start off with, what is a journalist these days? Would you include bloggers? Would you include someone live-tweeting this Committee who is effectively a member of the public? Where might we draw that line?

Andy Smith: To go back to what you were saying, there is an interesting debate to be had on that. I have seen various definitions. The advantage of PACE is that it does not define a journalist, and in some ways that is safer. If that definition is to develop as the technology develops, I would rather see that debate happen as a matter of developing case law, which would involve open hearings rather than conversations behind closed doors that make decisions arbitrarily, or not arbitrarily, about whether somebody who, for instance, had a regular blog and followed our own code of practice but was not paid for it would be described as a journalist. Frankly, some very good journalistic work is being done on the internet by people who are not associated with the traditional media outlets. There is a debate to be had there, but I would say it is developing.

Bob Satchwell: There are probably some common-sense definitions. It is difficult to define now, but, as Andy said, it will be developed in law. That is one of the reasons why there needs to be an ability to argue a case and say whether this person is a journalist or not. That is part of the principle that is there. I can see that some authorities would say, "We did not know he was a journalist. We just did it". That is the difficulty: that people will try to go outside what has been accepted practice in the past. It would be difficult to define absolutely what a journalist is.

Matt Warman: Bearing in mind that as-yet-undefined elasticity, how could we amend the Bill in front of us to achieve some of the things that you are talking about?

Bob Satchwell: There will be a submission from the Media Lawyers Association, which will come back in huge detail on this. Please excuse me for not having all that legal background. They will come up with some very clear suggestions on that.

Matt Warman: Mr Smith, did you want to add anything to that?

Andy Smith: Like Bob, I am not a lawyer. I would not want to start amending it for you, but the principles would involve something like "somebody who is regularly practising" or "employed". Those sorts of phrases would allow you to separate out those who are simply expressing an opinion on a blog on a regular basis from those who are engaged in journalism.

Q144 Mr David Hanson: Could you comment on what happens when a journalist is undercover and is acting as a journalist but is not, to the public knowledge, acting as a journalist at that particular time? The fake sheikh has been mentioned, but there may be other examples that we are aware of. I am interested, again, in the definition in relation to the Bill.

Bob Satchwell: In most cases, they will be employed or commissioned to be doing something undercover, and there will be some governance surrounding that from the person who has hired or commissioned them to do it. There are some difficulties if people are just going off on their own and doing it—difficulties for themselves, indeed—and they do not have the protection of an organisation behind them. That is what normally happens.

Andy Smith: The NUJ code of conduct is very clear in stating that investigations should be done by open means wherever possible and that any subterfuge has to be justified in terms of an overarching public interest, so you cannot simply decide to go away and pretend not to be a journalist because you feel that it will be the easiest way to get hold of the information.

Bob Satchwell: It is covered by virtually all codes across the media that you have to have a very good reason for subterfuge. In the new editors' code at IPSO, it is very clear that there is governance on that: at every stage of involvement in an investigation of that kind, notes have to be taken at the time about what the public interest was. It will be recorded and they will be audited on that.

The Chairman: Thank you, all four of you, very much indeed. It was very informative and very useful, and the Committee will be looking carefully at the written evidence that you will be providing us as well.

Rachel Griffin, Director, Suzy Lamplugh Trust (QQ 197-206)

Evidence heard in public Questions 197-206

Oral Evidence

Taken before the Joint Committee

on Monday 21 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Suella Fernandes MP, David Hanson MP, Shabana Mahmood MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Lord Hart of Chilton, and Lord Strasburger.

Witness: **Rachel Griffin**, Director, Suzy Lamplugh Trust, gave evidence.

Q197 The Chairman: A very warm welcome to all three of you. Thank you so much for coming along so close to Christmas. We are very grateful. As you probably know, the way the Committee operates is that we will ask you a number questions, which we hope will give you the opportunity to make whatever points you want. I will open by asking you a very general question and in each of your replies please feel free to make anything you like by way of an opening statement. What do you think of the draft Bill? Do you think it strikes the right balance between safeguarding our civil liberties and crime prevention? Perhaps we can start with you, Ms Griffin.

Rachel Griffin: I should start by saying that I am from the Suzy Lamplugh Trust. We run the National Stalking Helpline. A large proportion of the people who we help each year are affected by digitally-assisted stalking of some kind or another. The first thing to say about the draft Bill is that it is definitely necessary, from our point of view, for the police to have access to communications data to investigate many cases of stalking and cyberstalking. It is certainly necessary for the police to be able to access communications data to investigate and detect crimes. However, the point we want to make is that legislation should be only one part of a strategic plan to address digital offending. On a day-to-day basis we are finding that the police often do not make very good use of the legislation that they already have available to them. Our question would be whether a change in legislation would have an impact on the experience of victims on a day-to-day basis. On whether the Bill strikes the right balance between safeguarding and civil liberties, I defer to other organisations to answer that question. Our point of view is very much on the experience of victims of stalking.

The Chairman: That is what we would expect it to be.

Rachel Logan: Amnesty very much welcomes the opportunity to be here. We very much welcome having a draft Bill of some kind, because we are one of those organisations that has been saying for a long time that the existing statutory framework in this area is not up to scratch. Unfortunately, we are very disappointed by what we see in the Bill that has been put forward. To touch on a very small number of areas, given the time available, first, we see in the Bill not one, not two, but five sections dealing with bulk, indiscriminate collection

of or interference with individual privacy. From our perspective, that simply does not strike the balance or draw the line in the right place. We even see some targeted powers shading into what we would see as bulk powers in the case of thematic warrants.

I move on to intelligence sharing, which we have been litigating on for more than 18 months in the Investigatory Powers Tribunal. It has been the subject of at least two rulings. We were very surprised to see in what bare terms it is dealt with in the Bill, given how big the subject area is. We would have liked to have seen a clear, accessible framework, dealing with how material is received and sent overseas outside the MLATs. We would have liked to have seen that limit and not include the product of bulk interception either way—going from the UK or coming into the UK.

On oversight and judicial authorisation, unfortunately, we are disappointed by the judicial authorisation, or judicial review process, as it is put in the draft Bill. It does not amount to proper, independent judicial authorisation as is required for human rights compliance. It is simply not there. On the oversight provisions, similarly, having been through the IPT—I hope that I will get the opportunity to expand on this—we are very disappointed to see only one real substantive change to the way the Investigatory Powers Tribunal does its job. We would have liked to have seen a much more thorough look at how that works and whether it is properly independent and effective.

Finally, to touch on special protections in the Bill, again, this is an area that Amnesty has been litigating on in terms of legal professional privilege in the Investigatory Powers Tribunal, where we saw a concession by the Government that their entire regime in this area had not been human rights compliant. We saw a further finding that one of our co-claimants' legally professionally privileged material had been unlawfully retained. It is very disappointing to see nothing on the face of the Bill to deal with that properly, to deal with journalists, or even to consider giving further protections to human rights NGOs, such as ourselves, who we now know have, disappointingly, been specifically targeted for surveillance by the state. With all of that in mind, and there are many other areas that we simply do not have time to get into at this stage with the time allowed for the Bill process, we are very disappointed with what we have been presented with.

The Chairman: Thank you very much. Of course, every organisation, including yours, is very much entitled and welcomed by us to submit written evidence in detail.

Rachel Logan: We have done, this morning, for which we are grateful.

Alan Wardle: Good afternoon. Another fact that is relevant for this is that the NSPCC runs ChildLine, which you will all be aware of. It is now in its 30th year. Increasingly, children, as the Committee will know, are leading their lives online. More than three-quarters of 12 to 15 year-olds have access to a smartphone. That also means that many of the crimes committed against children increasingly have an online element. In particular, some of the ones I want to focus on are what you might call the harder-end cases, such as the possession, distribution and manufacturing of child abuse images, so-called child pornography, which is growing, and also cases of grooming of children, much of which is done online. More than 500 children contacted ChildLine last year about grooming and more than 80% of those cases had an online element to it.

From our perspective on the Bill, the most important thing for us is to ensure that the police have the powers that they need to track, investigate and prosecute these offenders. We are coming from a different place from Amnesty, which is more about bulk surveillance; we are more focused on specific criminal investigations that the police need to undertake. We have a particular concern that Clause 47 might be restricting too much the police's ability to investigate in what can be quite complex investigations.

Another point I want to make is that ChildLine has a very high level of confidentiality, but it has to breach children's confidentiality around 10 times a day, generally because those children are actively suicidal. Most children contact ChildLine online these days, so we need to ensure police can get those IP addresses quickly and actively intervene to protect those children. The two aspects that I would like to talk about are criminal investigations and ensuring police have powers, and an emergency function to protect a child's life if they are in immediate danger.

The Chairman: Thank you, all three of you, very much indeed for those opening remarks.

Q198 **Mr David Hanson:** The police's case, as put to us by Keith Bristow of the National Crime Agency, is that the Bill brings us up to speed with "what we need to be able to do in a digital age compared to an analogue age". Do you agree with that, or do you think the Bill goes further and adds new powers for the police?

Rachel Griffin: I smiled because I can see why that statement was made in theory, and it might well apply to cases of, for example, child sexual exploitation, where the focus is on intervention and stopping criminal activity escalating. From a stalking point of view, the key use of communications data in cases that we deal with is on investigation and detection in individual cases where the activity has already happened. We tend to find that it is not so much a case of whether the police have the powers; they already have a number of powers but we find that they simply are not being used in practice. For example, we often hear from victims of stalking who have been told to turn off their computer—"If you don't look at the emails it won't affect you"—or they might be told that that it is too expensive to investigate digitally, or that there is no point as the service providers will not be compliant, et cetera. For example, recently a caller to the helpline reported being told that police only access phone records only in cases of murder. There is a huge gap between what is going on in practice with regard to making use of existing powers and what may be envisaged in terms of the potential of the Bill. That is why we would like to see the police using their current powers to full capacity, as is reasonable and proportionate, but also to focus on not just legislation but the capability and capacity of police forces to make use of that legislation.

Rachel Logan: I will leave this to my colleagues at this stage.

Alan Wardle: The police's view on powers is quite important. From our perspective, we understand from the NCA that there has been a gradual erosion of the amount of data that they have been able to gather over the years. The Bill is very important to put that in place and to ensure that it is adaptable. Who knows what technologies there will be in five to 10 years' time, but the Bill has to have sufficient flexibility to adapt to those things.

On Clause 47(4), which has additional restrictions on granting authorisation, we have had initial conversations with the police and they have expressed concern about it. It would seem to us perverse if the data providers were able to hold all the information but the police were unable to access it. My understanding is that if people were conspiring over the telephone the police would be able to have all that information, but not if it was done online. That subsection talks about where the activity is mainly or wholly acquiring material the possession of which is a crime. Something such as possessing child abuse images is clearly a crime, but we know that for grooming cases where a lot of people are involved and it takes a long period of time, where, for example, a person books a hire car in place A and drives to place B or they book a flight, those factual issues, while not a crime in themselves, can help the police to investigate. It would be worrying to us if anything restricted the police's ability to investigate thoroughly along all the different strands of investigations. We would want to ensure that there is parity across the board and that the data the providers hold can be accessed by the police force for specific investigations.

Mr David Hanson: The question to all of you is: are the police powers under existing legislation proportionate and effective? Will they be more proportionate and effective under the proposed Bill, or will they be neutral or less effective? What is your view as to the police-central cases: do we need the Bill to update what we currently do? Is that right?

Alan Wardle: Yes it is, but my understanding is that this clause in particular would place a restriction on them that is not currently there. That would need to be worked through to see why it has been put in there and whether it will actively hinder the police's investigation of the kind of complex cases that I am talking about: the production of child abuse images, which, again, are quite often done by conspiracies, and online grooming. Yes, the need to have these additional powers is quite clear.

Rachel Logan: I am afraid that the question of police powers is not something that Amnesty can assist the Committee with at this point. It is not a part of the Bill that we have assessed or been involved with to date.

Mr David Hanson: With due respect I think that that is copping out of an answer. If the Bill goes forward, is Amnesty satisfied that the current proposals by the police are modernising their view based on the Bill? Ultimately it is about police powers and whether they are effective and proportionate. Surely Amnesty has a view on that.

Rachel Logan: With respect, it may be seen as copping out, but we are talking about a Bill of many hundreds of pages and many parts. Amnesty is a worldwide movement that focuses on many different aspects. We simply have not assessed those parts of the Bill yet.

Mr David Hanson: So you do not have a view on whether these current proposals are proportionate and effective.

Rachel Logan: At this point I do not have a view that I can assist the Committee with on the police powers in those parts of the Bill. I can help you, as much as Amnesty can, with questions of necessity and proportionality around bulk interception warrants, the structures around targeted warrants, and what is in the Bill on intelligence sharing, but I am afraid that the question of police powers and dealing with crime simply is not something I can help you with.

Mr David Hanson: Ultimately those are police powers. The question is whether they are proportionate and effective in relation to what the Bill proposes.

Rachel Logan: I am afraid that this simply is not something that we can assist you with. Those parts of the Bill go into Parts 3, 4 and 5. There are multiple parts of the Bill. We have not had a significant amount of time and they are not core areas of focus for us at this point.

Mr David Hanson: May I respectfully suggest that, when the Bill comes before both Houses of Parliament we would want a view on those issues? They are central to the Bill.

Rachel Logan: It may well be that, when we have had considerably more time and when the Bill goes through the proper processes, we will turn to that. I simply cannot say at this stage whether that will be Amnesty's focus.

Rachel Griffin: Our view is that it is unlikely—or that we are yet to be convinced—that the Bill will have an impact on the majority of cases of stalking as we experience them. That is not because data communications are not needed, but because the expertise in digital investigation and recognising risk is not as widespread in day-to-day policing as it needs to be.

Q199 Suella Fernandes: This is a question to Rachel Griffin and Alan. Can you walk us through a typical harassment case—if there is such a thing—or a child sexual exploitation or a grooming case, and how communications data would be helpful in identifying perpetrators and securing a conviction?

Rachel Griffin: From a stalking point of view, around 70% of people who call the National Stalking Helpline report experiencing at least one form of stalking behaviour that may require police to access some kind of communications data. Some 39% have received phone calls; 30% have received emails; 36% have received texts; and 37% have experienced stalking via some kind of social networking site. It is right that you made the point that there may not be a typical case of stalking because each one would be quite different. They are incredibly diverse in how long the stalking goes on for; some will be stalked for about six months, but, sadly, we have a small proportion of people who have been stalked for a number of years.

What tends to happen is that somebody will be stalked through a blend of different means. That may include physically turning up at someone's workplace or at their home, perhaps sending them letters, but also saying things about them via social media. Some will know that they are being stalked and that the activity is taking place online, but they do not necessarily know who it is, or there is a suspect but it is very difficult for them to prove. They will go to the police and say, "This has been happening, I've been receiving these text messages, these things have been written about me on Twitter". In a case where there may have been a number of text messages or emails, the police may need to identify that it was in fact a perpetrator—an identified individual—who sent them. That is where communications data may come in. Unfortunately, that is where we have too many examples of victims saying that they have gone to the police and found that, in some cases, the police do not even understand what an IP address is. The level of understanding is relatively low. That is alongside those cases where people say, "Well, come back when he

does something", suggesting that if it happens on the internet—if the stalking is cyberstalking—it is not real stalking.

Alan Wardle: It varies in grooming. Sometimes it can be one person grooming one child, or, as we have seen in some high-profile cases, it can be gangs of people communicating with several children. The process of grooming takes time, by its very nature. It lures children in, makes them feel good about themselves, offers them enticements, et cetera. We know from the National Crime Agency that the vast majority of cases involving grooming are online. That could be through social media, by various apps, by text message, by phone et cetera. Quite often, one of the challenging things around this is that children do not even recognise that they are being groomed—they think that it is their boyfriend, for example. The child will not necessarily keep the evidence themselves; they will not hold on to it. The police need to be able to identify from all those different sources what happened, to try to get a picture of who said what to who, where they were, who they communicated with, when they did it, et cetera, to build up a picture of what is going on, which obviously would go alongside personal testimony. That is why the point that Rachel Griffin makes is valid: we also have concerns about the police's capability—particularly that of local forces—to investigate and understand these offences properly. The cornerstone to that is having the information available to them so that they can identify what has happened, build up a picture of what is going on and investigate and prosecute these crimes.

Q200 **Baroness Browning:** Are the three purposes for which law enforcement can seek internet communication records the right ones? Should they also be able to use them for other purposes—for instance to locate missing people—even when no crime is suspected? We have received evidence from the police that much of their time is taken up with trying to identify vulnerable people, not necessarily because they have fallen foul of serious crime, but speed is of the essence because they are vulnerable.

Alan Wardle: On the first part of your question, as I mentioned, certainly on Clause 47(4)(c), which is the limitation where a person is "making available, or acquiring, material whose possession is a crime"; at first glance, and having had an initial discussion with the NCA, we are concerned that that might be too limiting. Using grooming as an example again, hiring a car to transport a child from one part of the country to another is not a crime in and of itself, but it is evidence of a crime having taken place. It would be worrying to us if that data was held by internet service providers but the police could not access it because it was not illegal material. More needs to be teased out throughout the process about what that means and what limitations that will place on the police.

On the emergency bit, as I said, ChildLine has to do this about 10 times a day. We work with CEOP very closely. The ability of the police to identify and rescue actively suicidal children who may not want to be contacted by the police is a very important function. We certainly would want to ensure that that capability is not eroded in any way.

Baroness Browning: Not eroded, but as drafted, will it not add anything to resolve the problem of your 10 children a day?

Alan Wardle: I spoke to a barrister about this last week. Her initial view was that Clause 46(7)(g), "for the purpose, in an emergency, of preventing death or injury or any damage

to a person's physical or mental health", would cover this situation, but again, it would be useful for the Home Office to clarify whether, in its view, that would cover it.

Q201 Lord Strasburger: Ms Logan, you mentioned in your opening remarks that one of the five areas you are concerned about is intelligence sharing. There is very little in the Bill about it and so far the Committee has heard very little about it. Would you care to expand on what Amnesty's concerns are and what advice you would give the Committee on it?

Rachel Logan: Yes, thank you very much. Amnesty has been engaged, together with Liberty, Privacy International and several other NGOs, in litigation in the Investigatory Powers Tribunal—it will now be off in the European Court of Human Rights in Strasbourg on this subject—to look at the way the UK both sends information, intelligence product, overseas and receives it from overseas powers. In the Bill we have very little at all on what are called "overseas arrangements". Clause 39, "Interception in accordance with overseas requests", provides for that activity, but simply talks about lawful interception being something, "carried out in response to a request made in accordance with a relevant international agreement by the competent authorities of a country or territory outside the United Kingdom". The only definition you have for a "relevant international agreement" is, "an international agreement to which the United Kingdom is a party". On the other side of the coin, when we think about what the UK is requesting others to do—perhaps not requesting, but what information it might receive from other powers—all we have in the Bill is a bare reference in Schedule 6 to a "code of practice", which, it is said, will be forthcoming and which will deal with the "provision about the making of requests ('relevant overseas requests') for intercepted material or related communications data that has been obtained by an overseas authority by means of any interception", et cetera, with no definitions of what any of this might be and no expansion on what any of this might mean. There is then further provision for arrangements to be in place around receipt or sending of such information, with no explanation of whether such arrangements will be public, what they might contain or what they might be.

We were talking about the product of bulk interception, such as, in the US, the product of Prism or the upstream programmes where material has been collected in bulk. We are considering a situation where we have a ruling in the Investigatory Powers Tribunal case that recognises that, until this litigation, any such intelligence sharing was unlawful because there was no policy whatsoever in the public eye in this area. All we got during the litigation was a small summary, which was corrected on many occasions, of what the arrangements in place might be. It was very bare bones. There was lots of talk about signposting to what was under the waterline. When we were in that situation we had very much expected the Bill, in the spirit of transparency, to provide a clear legal framework. Those simple references simply do not do that. How can Parliament and the oversight bodies provide proper scrutiny? How can the public understand where their information might end up or what might be being looked at overseas if there is simply nothing there? That is very disappointing.

The Chairman: I think we will touch on that in further questions as well.

Q202 Dr Andrew Murrison: Amnesty obviously has an international perspective. I am interested in your view on whether this legislation is compatible with the direction of travel

taken by countries with which we can reasonably be compared, in particular the other four members of the "Five Eyes" community.

Rachel Logan: I want to be very careful about what I say on that topic at this point because there is a certain state of flux in the relevant "Five Eyes" countries. I would be very happy to come back to the Committee with a more detailed analysis. I will say that in the US, for example, we have recently seen, as I am sure you are aware, changes around the Patriot Act and the Freedom Act and a certain amount of rolling back, but I would not want to give the Committee any precise answers without being able to go back to that in more detail. I would be happy to do so.

Dr Andrew Murrison: It would be quite valuable if you could as part of written evidence. As we have been going through this there have been comparisons with the "Five Eyes" community, with whom, of course, we share data. It would be useful from your perspective as an international organisation to provide some insights if you could.

Rachel Logan: I will certainly see whether we can do that in the time available.

Dr Andrew Murrison: Thank you very much. May I ask you about communications data? A lot of what we have been dealing with over the past few weeks has to do with the times permitted by the Bill—for example, five days for judicial review warrants issued by the Home Secretary and 12 months for the retention of communications data. I would be interested in your thoughts on whether 12 months is right—in particular, to nuance that slightly, whether that 12 months might be amended upwards or downwards depending on the situation, on the crime that we think has been committed and on the circumstances, thinking of missing people, for example.

Rachel Griffin: We would resist offering an arbitrary time limit, which I dare say is not terribly helpful. From the National Stalking Helpline's perspective, we tend to talk to people at the very beginning of their journey through the criminal justice system. They may not even have reported the crime when they talk to us. I would advise getting evidence from people such as the CPS and the police on how long it takes for a prosecution to come to court from that point of first report. That will have an impact. It will not be terribly helpful to have a time limit that may have expired when the evidence is finally gathered and a prosecution is pursued.

Also, it is worth bearing in mind how long people have been stalked for. Some 48% of the people who talked to us have been stalked for longer than one year. That suggests that there might be a need, by the time a victim goes to the police, to go back some time to find some of the essential data. It is also really important to understand why people do not come forward, whether it is to do with cyberstalking, or, in the context of stalking, things such as revenge porn. Often people will not come forward because they do not feel that they will believed and they do not have the confidence to talk about their experiences.

Also, it is vital to point out that, in preparation for this session, we contacted the Home Office to ask how many investigations are impacted by lack of communications data—we do not know what we do not know. The feedback was that it is impossible to know how many criminal investigations are impacted by a lack of available communications data. Again, I come back to the point that we definitely recognise the need for communications

data, but we do not know the size of the problem that we are trying to solve with the Bill. Therefore, it is difficult to determine whether the existence of the data would be helpful and for how long that data would need to be kept because we do not know how many prosecutions are not going forward without that data. It feels very circular.

Dr Andrew Murrison: Where do you think the Home Office got the figure of 12 months from, then?

Rachel Griffin: I am not sure. You would have to ask the Home Office.

Alan Wardle: My understanding of the 12 months was that the last time this was legislated for Parliament took the view that that was the appropriate time. Any flexibility around that ought to be evidence-led. Certainly, we know that some of the more complex cases, some of which I have alluded to, take a long time to build up the case. We hear from the police of cases where, because it is a rigid 12 months, as the case proceeds bits of evidence fall off the end after a year. We need to know whether there is any flexibility around that once a case has started. On disclosure, again, similar to the point that Rachel made, not all children disclose immediately whether they have been abused. They can take time. It is a judgment for Parliament to make. It ought to be evidence-led and take a view on whether there are more serious and complex crimes where data need to be held for longer and how that would work.

Dr Andrew Murrison: I can see why organisations such as Suzy Lamplugh Trust and the NSPCC should want the police to have these powers since you are faced, on a day-to-day basis, with very vulnerable people. However, do you have any concerns more broadly about the acquisition and storage of communications data and potential misuse of that material?

Alan Wardle: Yes. It clearly needs to be kept safe. Another thing to remember is that children are users of data as well and they will want to have their rights and privileges protected. Clearly, there have to be very strong safeguards around that. I am not a technical expert so I would not be able to tell you how that is done, but the data needs to be kept securely. It needs to be accessed in very strict conditions to give people confidence and assurance that the data is being used properly.

Rachel Griffin: I echo that. There will be a number of cases where someone who has been stalked will have their security, whether physical or online, compromised in some way. It is critical that they have confidence that their data will be treated appropriately.

Dr Andrew Murrison: In situations such as that of TalkTalk, are you confident that there are likely to be systems in place to guarantee people's safety and security?

Rachel Griffin: Guaranteeing safety and security is very difficult. It is particularly difficult when someone is motivated by the kind of obsession and fixation that stalkers commonly display. It would be completely wrong for me to say that I would have confidence that that can be guaranteed, but victims should have a reasonable expectation that their data will be kept as securely as possible.

Q203 **Lord Hart of Chilton:** I must disclose to the record that 50 years ago at university I joined Amnesty International.

The Chairman: You have disclosed your age as well.

Lord Hart of Chilton: I know—how youthful I still look. We have been supplied with the open determination of the Investigatory Powers Tribunal on 22 June 2015, from which we see that GCHQ retained material for longer than permitted under the policies. Therefore, there was a breach. My first question is whether, in the light of that decision, you are confident that there are sufficient safeguards in place governing the activities of the intelligence and security agencies. I rather think from what you said at the opening that you are not.

Rachel Logan: No, indeed. First, it is important to think about what that finding tells us and then look at whether we feel that the safeguards are sufficient in the light of that. It is important to understand that Amnesty found very little out from that determination. I can come back to the question of how we got it, which sheds rather a lot of light on our views on the Investigatory Powers Tribunal, but it tells us very little at all. We do not know why our communications were intercepted and selected for examination. We do not know what was looked at and when. We do not know what policy was breached or in what way. We do not know whether this was a one-off and just confined to us, or whether it is systemic among other NGOs that were not involved in the litigation. We have had no ability whatsoever to input into the conclusions of the tribunal because we were excluded from the hearing that resulted in that determination. That begs the much more important question, as far as we are concerned, which is why human rights NGOs were being targeted for surveillance in the first place, quite aside from whether our material was retained for too long. The other NGOs in the same legal action received a simple one line, "No determination in your favour", which does not tell them whether they were intercepted, or whether they were intercepted but the tribunal considered it to be lawful, et cetera.

It is a very sparse determination, but what that tells us about the safeguards and the oversight system is that something has gone very badly wrong. It appears that this has been considered an acceptable activity by the Secretary of State and all those others involved in oversight during the process, because we know that we were picked up under a general warrant. It appears that this is something that was carrying on which either nobody raised any objection to because they all thought it was fine and dandy to be spying on human rights NGOs and did not know about the specific policy breach, or they knew about the breach and did not consider it to be important. We do not know why this was not picked up until we got into a tribunal process. It is very worrying that we had to get to that stage to get this finding.

The same applies to the other litigation we have been involved in—the legal professional privilege one I alluded to earlier—where one of our co-claimants found that his legally privileged communications had been picked up. That is a really frightening proposition for those of us who have been involved in the legal system for a long time. Again, he was not able to contribute to the hearing where the finding was made that this was not very important. From our perspective, something needed to change with that in mind. We have not seen that something in the draft Bill, particularly if you look at the retention provisions in it. Data can be retained as long as it is necessary or "likely to become necessary" to retain it. That is stunningly broad. It is very worrying for us, having been in the position of having had our data retained and having been spied on, that we do not have more safeguards in

this. I can come on to look at the IPT and the judicial relation if you would find it helpful, but basically, against that background, there does not seem to be enough.

Lord Hart of Chilton: What further safeguards do you think are necessary?

Rachel Logan: It comes back to the question of definitions. There are incredibly broad definitions around purposes in the various warrants. There is no definition of national security. Just recently, a decision by the Grand Chamber in Strasbourg, I think last week, said that it is important to have tighter definitions than just "threats to national security" when we talk about warrants of this kind. You have these very broad definitions and general purposes permitted as a basis of interception. Then you again have a complete absence of proper judicial authorisation. In Amnesty's view, this so-called double lock does not amount to a human-rights-compatible process. The decision is still being taken by the Secretary of State. It is merely being reviewed on judicial review principles by a judicial commissioner. If Clause 19(2), which states that this must be done to a judicial review standard, was not intended in any way to limit the scope of the review undertaken by the judicial commissioner, then it is unnecessary or unnecessarily complicating the situation.

Our view—like, I am sure, many of the other NGOs you have heard or will hear from—is that that is simply unnecessary if the intent is to have a full, merits-based review by an independent judicial authority before a warrant can be issued. We would like to see that happen. We would like to see strong post facto oversight done by different people than those involved in the authorisation process. This melding of the oversight and authorisation functions with the judicial commissioner is something that worries us. Down the line, looking at the Investigatory Powers Tribunal itself, I have spent nearly two years now litigating in this tribunal alongside some very well-known QCs from my old chambers and elsewhere who are well-versed in SIAC and other places where there are secret processes and unusual court systems. This court and these processes are the most frustrating and obfuscating that I have ever encountered in the UK system. We are talking about situations where, whether for intent or not—I am sure not, because everyone wishes this to be open—the bias is towards secrecy and not letting the claimant in to what is ultimately a determination of their rights and freedoms. That needs to change. All we have here is an additional right of appeal. There has been no further look at the procedures of the IPT, which allowed the Government to argue this year that, even if the tribunal made a determination to favour individuals—that they said behind closed doors, "This person's rights have been violated"—they should not have to tell the claimant. They could lie and still say, "No determination in your favour". We had a whole hearing on that topic. In the end the tribunal rejected it, but there is that level of vagueness and secrecy in the tribunal's rules. That simply has no place in a rights-compliant oversight and authorisation system.

Lord Hart of Chilton: Do you think, then, that there should be a blanket exemption for legally privileged communications?

Rachel Logan: That is the basis in English law. This is not a question merely of human rights law, this is about the common law.

Lord Hart of Chilton: No, but in respect of this Act.

Rachel Logan: Yes, we do. All there is here is a provision for codes to be available. We have to look at the safety of the justice system, as well as rights and freedoms. This is the most sensitive and the most basic principle. If I cannot, as a lawyer, say to my client that what they are telling me is entirely confidential, how can I know that they will feel free and safe and able to give me full information? There is a significant chilling effect from the mere fact of interception of legally privileged communications that really needs to be taken into consideration.

Lord Hart of Chilton: You mentioned a moment ago the Investigatory Powers Tribunal. Do you think that the provisions there are satisfactory? Again, I rather gather that you do not and that you do not think that the Investigatory Powers Tribunal provides a satisfactory route for appeal and remedy.

Rachel Logan: Indeed. The judgment we received from the Investigatory Powers Tribunal on 22 June was not in fact the final judgment in that hearing. The judgment on 22 June said, "There has been no determination in favour of Amnesty International; that is, you have not been unlawfully intercepted. There has, however, been a determination in favour of the Legal Resource Centre in South Africa—a very well-respected NGO—and the Egyptian Initiative for Personal Rights". On 1 July, having had a period for corrections and clarifications to the draft judgment, none of which were put into effect by the Government, we received an email out of the blue from the Investigatory Powers Tribunal informing us that there had been a mistake and where the judgment said EIPR, it meant Amnesty International. That was following a hearing that supposedly was looking in the most detailed consideration at our rights and at particular communications that had been intercepted and whether that was lawful and proportionate. We asked, quite rightly, "How can this happen?", and asked for an open determination explaining how a mistake of this kind had been made. We received a very unsatisfactory response from the tribunal. Indeed, Parliamentary Questions have been asked about this by quite a few Members of the House—both Houses, in fact—seeking a Statement from the Secretary of State, asking whether other human rights organisations have been in the same position, and nothing has been forthcoming. That casts light on quite how problematic the IPT currently is. It needs to be sorted out.

When it comes to the Investigatory Powers Commissioner, we set out in our written submission that it is mostly things around the edges, around independence and effectiveness. We would like to see the oversight and authorisation functions separated. This is a small group of people and they will be looking at the full process to see if it has been gone through appropriately, and reviewing that. In our view, it would be safer to separate out the functions of overseeing the process and undertaking the process, even if it is just a part of it.

Q204 Matt Warman: I would like to ask a supplementary question. Were you saying that there would be a chilling effect if legally privileged communications were intercepted? As I understand it, that power has already been avowed and therefore theoretically it is already happening and lawyers and their clients might reasonably worry about it. Has there been a chilling effect, given that this is something that could theoretically happen already?

Rachel Logan: I cannot speak for the entirety of the legal profession, I am afraid, I am simply one representative of it—and from Amnesty, obviously. It has certainly caused enormous

concern to us in how we deal with our clients. Amnesty does worldwide research and litigation on a range of human rights issues, often right at the edge of the issues that Governments are uncomfortable with; for example, looking at the involvement of our own Government in rendition and abuses during the war on terror. But we are also very much concerned with Governments overseas. It is very difficult for someone intercepting our material under a broad warrant to distinguish between what might be country research material and what might be professionally privileged because it concerns witness statements, instruction, et cetera. We are very concerned about the impact of knowing that material which is legally and professionally privileged is being picked up in their net.

Matt Warman: So has it had a chilling effect on your own communications?

Rachel Logan: I am not quite sure what you mean by that. Are we extremely concerned and worried about what we say? Yes, we are.

Matt Warman: Has that changed since the power was avowed in this country?

Rachel Logan: There is always a difference between when you worry that something is happening and when you are told that it actually is happening so, to that extent, yes.

Matt Warman: Moving on to communications services providers, from an NSPCC perspective, are you worried that communications service providers co-operate sufficiently at the moment, when information could help the kind of work that you do?

Alan Wardle: Generally, things are pretty good. Looking at issues particularly of child abuse images and how those are disseminated across the internet, Google and Microsoft—at the instigation of the Prime Minister—did some really good work a couple of years ago which means that it is much more difficult to find those images through an open search on the web. Now, with some 100,000 search terms, you get only what are called clean searches; that is, they do not give those images. So that has been good. Most of the big companies are involved with the Internet Watch Foundation. Certainly in this country we are pretty proactive so if an image is found, it is generally down within two hours, so that is pretty good.

On the content, because the majority of the big companies are American, you would have to ask the police. I am not sure how the investigation of the content of communications is working. We have an issue with some of the internet hosting companies, such as online storage functions where people are uploading and storing a whole host of images. We think that that issue needs to be looked at in more detail and we are looking at it at the moment. Most of the companies recognise that this is a very serious issue and they are generally very co-operative. It is a global issue so, while the UK is very seized of this issue, we are seeing some alarming developments in other parts of the world—such as livestreaming of child abuse, which is crowdfunded—which is why these sorts of powers are essential.

Matt Warman: Will the Bill improve that situation or not make that much of a difference?

Alan Wardle: Internet connection records are very important, as I have already indicated. When it comes to the information that is needed, the current process is often very convoluted, when you have to go through the MLAT process. Anything that could be done

to simplify and expedite that would be good. We know from the police that they do not even bother to apply for evidence in some cases because they know it will take too long.

Rachel Griffin: We have had feedback from police officers we have worked with on the National Stalking Helpline that communications service providers are not always helpful in cases where the police need their assistance. But we do not really know whether this unhelpfulness is to do with reluctance to help, misunderstanding of what help is needed, or because the legislation needs to change. What is clear is that CSPs, as well as improving co-operation with law enforcement agencies, need to provide more assistance to the victims, who are often seeking help, advice and protection after being targeted when using their services. Again, it is very difficult to say whether the proposals in the draft Bill will improve that co-operation without having a better understanding of what the barriers are perceived to be by the CSPs themselves.

Q205 **Suella Fernandes:** I have a follow-up question for Amnesty. You talked a lot about privacy rights. Obviously, we have to strike the right balance but I heard very little about national security. We have heard a lot of evidence and we have on the public record that the head of MI5 has said that we face an "unprecedented scale and character" of terror threat at the moment. We have heard from witnesses about very serious crimes that are being perpetrated online. You obviously do not feel that the draft Bill is satisfactory but where do you think the balance should be struck in meeting this very important need to safeguard the public?

Rachel Logan: There is of course a critically important need to safeguard the public. That is part of human rights protection and we all have the right to life and security and all those sorts of things. That is part of what we are looking for as an organisation. But as you say, it is a question of proportionality and where you draw the line. For example, I am sure that it would be useful for crime prevention and national security purposes if we all had to go round with a body camera on, videoing where we were at all times, and had to hand that tape over at the end of the day, or if we had to keep a list of everywhere we went and everyone we spoke to, and handed that over. That might well assist in preventing more crimes, but for most people that would be an intolerable level of intrusion into their private lives. For us, the Bill simply does not draw that line in the right place. Targeted, suspicion-based surveillance is a very different world from what is being proposed here.

Suella Fernandes: When it is necessary and proportionate.

Rachel Logan: This is the question. "Necessary and proportionate" usually means the least intrusive measure that can be used to achieve a legitimate aim. That is precisely the question that we are all here to debate and we do not think that the Bill has that line in the right place.

Suella Fernandes: My question to you, Rachel and Alan, is this. The Anderson review described Tor as a facility that enabled the digital abuse of anonymous activism and dissident activity. What is your view of this Bill's potential effect on encrypted communications in the context of your work?

Rachel Griffin: I would certainly refer you to those with greater expertise than me on the digital side of things, but my observation about encryption is that stalkers and cyberstalkers

are fixated individuals who will use any means available to them. We have had a number of cases where victims of cyberstalking have had their devices hacked by stalkers, and in those cases we have advised them to use encrypted services in future. We have experience of encryption being used for both good and bad reasons. Obviously a balance needs to be found, but I do not have the expertise in encryption to answer that question in an informed way.

Alan Wardle: Tor is a place where quite a lot of the most dedicated—if you can call them that—people who perpetrate these crimes go, particularly in the production and dissemination of child abuse images. Essentially it is a challenge for law enforcement. Being able to identify the perpetrators is very time-consuming, and I do not think that anything in the Bill will necessarily affect that. It is one of those things, given the way the internet is designed. A third of internet users across the world are children, but the internet was never designed as a child-friendly place, and we are almost going around saying, "Can you put safeguards in at the beginning?" Would you design it in this way now? I do not necessarily know that we would, but we are where we are, and certainly from our perspective the key thing, as well as power, is law enforcement dedicating the necessary resourcing and skills to get officers to do the quite painstaking work of cracking these rings of people, which are global and are perpetrating some of the vilest crimes against children. We need to ask encryption experts about that, but it is certainly challenging for law enforcement and we need to make that it has the resources—the powers, the skills, the expertise—to be able to deal with these policing challenges in the 21st century.

Suella Fernandes: I have one last question on a point that both of you raised earlier. You mentioned suicidal children getting in touch with you as well as tracking and trying to pinpoint people who are involved in stalking. Can you give us an idea of the need for timeliness in securing warrants in those situations? When you are in the process of an investigation or trying to track someone down, do you operate in a series of days and months, or is it hours and minutes that you and the law enforcement services need in order to exercise your powers?

Alan Wardle: For ChildLine it is hours and minutes. Someone will be called at 4 o'clock in the morning to breach that child's confidentiality, if that is required. There are cases of the police literally cutting down children who are found hanging and saving their lives. I was in a meeting with one of my directors not so long ago. They had to authorise something; the police intervened to protect a child who was about to jump off Tower Bridge. In those cases, it is a matter of hours and minutes, which is why there is a need for the systems that we have in place in CEOP, which are very fast and rapid. If a ChildLine counsellor and their supervisor think that the child is in immediate danger, sometimes that speed is of the essence.

Rachel Griffin: This is an excellent question, because it really helps me to draw out the distinction, as I see it, between our perspective and an organisation that is working on child exploitation. Very rarely will we deal with a victim of stalking where there is not enough risk information for the police to put protection around that victim based on a fairly well-established stalking risk assessment protocol. It is very rare—I cannot think of an example—that the information to put that protection around that victim was dependent on accessing communications data. The communications data concerns on the part of the

victims we deal with come about when evidence is being gathered to support an investigation and prosecution retrospectively. Given where stalking tends to sit in the list of priorities in a number of police forces, particularly digital stalking, which is perceived as difficult to investigate, that is where victims of stalking will end up, I fear—often at the bottom of the list of priorities.

Q206 Lord Butler of Brockwell: My final question is to Ms Logan, if I may, following up Ms Fernandes's question. Is Amnesty International opposed to bulk interference per se?

Rachel Logan: It depends on how you think about that question. Do we think that bulk interception draws the right line in the sand? Do we think it is a proportionate way of dealing with the threat? No, we do not.

Lord Butler of Brockwell: So as things are, you do not agree with bulk interception at all.

Rachel Logan: As currently laid out in the Bill, we do not consider that bulk interception—indiscriminate, suspicionless surveillance—is proportionate interference into an individual's rights.

Lord Butler of Brockwell: What needs to be done to the Bill to make it acceptable to you?

Rachel Logan: I am afraid that I can only talk to the parts of the Bill that we have assessed so far. We would like to see the provisions on bulk interception warrants stripped out. We would also like to see a change to the section dealing with so-called targeted warrants, which provides for incredibly broad thematic warrants, changed and provided with much tighter definitions. We would like to see a return to suspicion-based interference, the suspicion-based surveillance of individuals who are properly identified and properly targeted, as we would do normally in normal, day-to-day real-world life.

The Chairman: Thank you, all three of you, very much indeed. It has been a fascinating session. Thanks for coming along, and happy Christmas to you.

Hugh Woolford, Director of Operations, Virgin Media (QQ 101-115)

Evidence heard in public Questions 101-115

Oral Evidence

Taken before the Joint Committee

on Wednesday 9 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Suella Fernandes MP, Mr David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Lord Henley, Lord Strasburger.

Witness: **Hugh Woolford**, Director of Operations, Virgin Media, gave evidence.

Q101 The Chairman: A warm welcome to the three of you. Thank you so much for coming along. You represent very significant companies with a lot of relevance for this particular Bill. Apologies to you for starting a bit later, but there was a vote in the House of Commons, which delayed our procedure. I am going to kick off the questions by asking you all to answer the one I am going to ask. If you want to say anything by way of a short general statement, perhaps you would like the opportunity so to do when I have asked the question. Again, welcome to you.

My question is a fairly simple one: how extensively is the Home Office engaged with you with respect to the provisions in the Bill? Perhaps Mr Hughes would start.

Mark Hughes: We have been consulted. We welcome the consultation that we have had. We have had a number of opportunities, and, overall, we are pleased with the level of consultation. There are obviously circumstances where it could be better and we could have done more, but, broadly speaking, it is very different from previous iterations we have had with the Home Office so we are comfortable with the consultation that we have had.

The Chairman: Thank you very much. Mr Kinsley.

Adam Kinsley: Indeed. I would echo that. There has been extensive consultation over the last months and it has been a marked improvement on last time.

The Chairman: Good. Finally, Mr Woolford.

Hugh Woolford: I would echo that. We have had engagement, and we have had high-level engagement both on the legal and operational sides. It is welcome that we are having that engagement.

The Chairman: That is a good start. Lord Butler.

Q102 Lord Butler of Brockwell: Following on from that, you are satisfied with the consultation, but has it led to agreement about what is practicable? Let me elaborate on that while you are thinking about it. This is on the nitty-gritty of how it is done. I am after whether

you think it is practicable to separate communications data from content, or at least the type of communications data you are being asked to retain, whether you are confident that you have the equipment that would enable you to do that, and whether you can give us some idea of what degree of extra costs that would impose on you. I hope that is not too much of a question.

Hugh Woolford: I will kick off and then pass across to my colleagues. I will take it in bits. On how easy it is to separate communications data from content, in the dealings we have had to date we feel that we need more work to get more clarity over what is considered content versus communications data. We need more workshops between the bodies to flesh that out. At the moment there are very high level—

Lord Butler of Brockwell: Excuse me, but does "bodies" mean the Home Office and the providers?

Hugh Woolford: Absolutely, yes. At the moment there are very high-level definitions. You could, for example, say that a route URL for bbc.co.uk is considered communications data, but if you put a "/news" on the end that may be content, so there are nuances—this is the way the Internet is constructed and used—that mean that does not always hold true. There are some general principles in place. We need to move forward and get some more detail in place around some of those nuances and how to handle some of them. That is the first point.

Leading on from that, given that we have not got to the nub of how we would differentiate, the answer is no, to be perfectly honest. We have early discussions going on with regard to some of the equipment or angles that we could look at, but there is a huge piece on volumes, which I am sure we will come to later in the session, that has a massive bearing on the equipment that we need and therefore also the cost.

Adam Kinsley: At this stage, we have to differentiate the conversations and the factsheets we have seen and what we are looking at in the draft Bill. The draft Bill is obviously very high level and it is not sufficient to be able to map across from that and understand exactly what we are going to need to do. By definition, it is going to have to come later in codes of practice and in further discussions. Going back to your question, to be able to differentiate and look at communications data within what are effectively packets of data, there will need to be investment in new types of technology for us to be able to get up to the first slash. The way the Internet is arranged and operated is not simple. We are going to have to look at individual use cases and understand exactly what we will need to do. Hopefully, that answers your question.

Mark Hughes: There are a number of parts to the question. The first is whether or not it is technically feasible to separate content from communications data. The draft Bill usefully defines communications data both from an entity and an event point of view, which is a new set of definitions, as opposed to the previous or existing regime—the RIPA regime—and then content. Technically, it is feasible to separate various parts of the packets; we can deploy tools to do that. The point about that is that, increasingly, especially in the future, with more and more encryption, the ability becomes more limited to take you back to purely an entity level piece of communications data as opposed to richer parts of communication data. That is the first thing.

More broadly, there is a lot of discussion, and has been, about definitions. We have already started talking about them today. It is important to look at definitions in the context of the level of intrusiveness that is the purpose behind the power being sought. That is always the reference point. The definition comes from the level of intrusiveness that is going to impact on our customers and on citizens generally. The definitions are derived from the level of intrusiveness to help bucket, effectively, certain types of data, be it first slash-type data or whatever it may be, to have a way of defining certain types of data. The caution I always put on definitions is that it is not easy to write them down, and we can see that right across the Bill, but with the additional checks and balances put into the draft Bill around legal oversight stuff, there is the possibility to refer back to the level of intrusiveness. Where the definition in the draft Bill might not be sufficient at the moment, there is the possibility through oversight to question that.

I think your next point was about whether or not the equipment exists. Yes, it does. There are various technologies available to us, although they are limited by the way in which the traffic is sampled, and there are many considerations around that. Indeed, some of the Bill, especially in the area of Internet connection records, which are new data that we have never collected before for that purpose, means that we will have to deploy new equipment to comply with the legislation as it is drafted. That comes at a cost. Clearly, there are two things about costs that concern us. First, it is not clear in the Bill at the moment that we will be eligible to recover all our costs, and we think that is important for two reasons. First, the mere fact of defining how much something will cost to meet a certain type of power will help to limit and frame the level of intrusiveness. In other words, an open-ended view of what something could cost could be problematic in the sense that capability could be stood up, which could cost a lot. Therefore, a proportionality check comes in through ensuring that it is clear that costs will have to be met. Secondly, clearly, if the cost is not met in that way, it will have to be found in some other way. There will be additional costs and we certainly have some views on some of the calculations—perhaps we might talk about that later on.

Lord Butler of Brockwell: When agreement on definition is reached, how do you envisage that it will be expressed in statutory form, or would it be expressed in statutory form? Would it be by a statutory instrument or will further amendments to the Bill be necessary?

Mark Hughes: This process, through scrutiny, is in part helping to tidy it up. There is, I believe, much more work to be done to ensure that we get tighter definitions where we can. Equally, as in my previous point, we have to ensure that the oversight regime allows us the ability to discuss that. More specifically, to answer your question, the codes of practice, which we look to see before the publication of the final Bill, will go some way to clarifying a lot, as well as the oversight instruments that exist in the draft legislation, which will allow us, if we are not comfortable with that, to visit it with the appropriate authority.

Q103 Lord Strasburger: Gentlemen, you have mentioned encryption as being a complicating factor. We have also heard in previous sessions that the way the Internet is increasingly being used—for example, with a Facebook page—is as a smorgasbord of content and data, and that it may be impossible to separate them automatically. I doubt that you would fancy doing it manually. How are you going to cope with that problem?

Adam Kinsley: You have put your finger on the nub of the technology challenge. When you are requesting a page within Facebook, facebook.com/spurs, or something like that, you are going to get lots of different content delivered: you are going to get the league table, the Harry Kane goal or something like that—lots of data. We need technology to analyse all of that, match it all up and work out which bit is the first slash. It is a big technology challenge. As Mark says, it is not impossible but it is very expensive.

Lord Strasburger: Thank you.

Q104 **Dr Andrew Murrison:** Obviously, there is some urgency to all this because the Home Office would rather like to get cracking with gathering the information that it says is necessary to safeguard security and deal with serious crime. I am interested to know from you how long you think it is going to take, given the technological challenges that you pose, to get to that first slash point.

Hugh Woolford: We have put some thought into the timescales. As long as the necessary discussions and detail were worked through, we feel that we could probably start in 2017, with earliest deployments in 2018, depending on the requests and the scale. Those are the sorts of timescales that we would potentially be working to.

Dr Andrew Murrison: That sounds quite a long timeframe to me. Does that match the level of patience that you perceive in your dealings with the Home Office, or is it disappointed by that?

Hugh Woolford: I honestly cannot comment on that. Those are the timescales that we have in mind. That is currently where our heads are.

Dr Andrew Murrison: I have to say that the definitions on the face of the Bill confuse me; I suspect that they will probably be rather clearer to you since you are in this particular business. I have heard from you already that you value the improved definitions, particularly those in Clause 193, which I guess is what you are referring to when talking about entity data and events data, but I am also hearing that you expect further clarification by way of codes of practice. Where do you think we are at the moment with the definitions? Where on a Likert scale of zero to 10—where zero is completely useless and 10 is perfection—do you think we are at the moment?

Adam Kinsley: I am not sure that the intention is for us to be able to deliver any capability based on the face of the Bill alone. As it stands, it is pretty close to zero, I would say. We absolutely need more detail to be able to deliver. I am not sure it was the Home Office's intention to be able to deliver based on the definitions on the face of the Bill, but that is obviously a decision for Parliament—how much goes on the face of the Bill, how much goes into codes of conduct.

Mark Hughes: There has been a lot of work to help to clarify a number of the definitions in the Bill. In the Internet connection records space, for example, it is difficult for us to comment because we are not defining the purpose for which it is intended. Therefore, by its very nature, I am not in a position to comment. There has been a lot of work. As we have already said, there needs to be more work and the codes of practice should support that.

Adam Kinsley: I should qualify my comments. I was answering in relation to Internet connection records primarily.

Hugh Woolford: I would echo that.

Q105 **Mr David Hanson:** Page 25 of the draft Bill, regarding Internet connection records, says helpfully: "A kind of communications data, an ICR is a record of the Internet services a specific devices has connected to, such as a website or an instant messaging application. It is captured by the company providing access to the Internet". Is that your understanding of what an Internet connection record is?

Hugh Woolford: Today we do not have anything like an Internet connection record. This is something that is completely new for us, and I have looked at previous Bills. From a business point of view, there is no need for us to capture any of this information. We do not have what could be classed as an Internet connection record.

Mr David Hanson: I am a layman here, so tell me how hard it is to collect one of those, to establish it.

Mark Hughes: On the face of it, it sounds like a relatively straightforward thing to do. In some respects, the Bill goes on to define the purposes for which they are being collected, and three purposes are outlined. They are obviously around the person, illegal content and the service, broadly speaking. It helps as well when you combine the two things; you take the initial definition and the purposes that are in the draft Bill, and that has given us a route to analyse what would need to be collected—as Hugh said, it is not something that we collect today—to fulfil that definition and then have data available if that were to be the case for that purpose. You would have to look at quite a lot of data to be able to achieve that.

Adam Kinsley: If you think about what a CSP would be required to retain at the moment, essentially you may be given an IP address that would be applicable to your computer for potentially up to a week and that would get recorded once. There are a couple of bits of data that would be recorded for about a week. In what the Bill is seeking to do, first of all you would have to analyse all your Internet sessions in that week—in fact, throughout the whole year—which would obviously be quite a lot; in the Facebook example we used earlier, just one request to a Facebook page will come back with lots of information within it that needs to be matched. You need to analyse all that, match it all up and then retain the bit that the Bill will ultimately end up with. The magnitude of data collected that would be processed would be massively more and the magnitude of data that would then be retained would be tenfold, a hundredfold more than we collect today.

Q106 **Mr David Hanson:** At the moment we are considering the draft Bill; it is going to go through the House of Commons and the House of Lords and be law by September or October next year. How long is it going to take you to establish the mechanisms? How much is it going to cost you to establish the mechanisms? Who do you think is going to pay for this? Is it the taxpayer, as in all of us? Is it you or a mixture of both? If so, what is the mixture? Is it practicable? Is it going to do what it says on the tin? We need to get a flavour of this from you.

Mark Hughes: Let me go through a number of those things. There is a spectrum of options available on Internet connection records in terms of the amount of coverage. The Home

Office has consulted us and we have had a pamphlet that has been issued about Internet connection records, with some view of costings. We have obviously done work based on the assumptions. The assumptions from the Home Office are that it wants as broad a coverage as possible to achieve this, which is going to be costly. We have worked up some assumptions and indicative costing.

Mr David Hanson: Are you able to share that with us or not?

Mark Hughes: Yes. The publicly stated figure, I think, from the Home Office is that it has set aside £174 million for this. We have worked out that for us alone—I cannot comment for others around the table or others in the industry—to fulfil the assumptions that we have been given will cost us tens of millions, so the lion's share of that £174 million would be for us alone. How others would do it depends on how they manage and architect their networks. We have looked at it. As to the implementation time that it would take, again it depends: there are some things where extant capability could be used to gain some coverage relatively quickly, but to fulfil the assumptions we have been in dialogue with the Home Office on, it would take longer to deploy equipment comprehensively across our network—deep packet inspection equipment—to be able to generate the data to then have them retained to comply with the legislation.

Hugh Woolford: On costs, we broadly agree. Our teams have had a look at the high-level information we have and think similarly—tens of millions. I would love to give you an exact figure. We are not saying it cannot be done. Anything can be done in this space with enough time and money. We have a broad set of requirements, but to enable us to move forward we need to bring some more specificity to those so that we can start giving more accurate estimations of costs and time. Depending on how much you are trying to capture and across what frequency, one big piece of it is how much of whatever the equipment is you might need to deploy; therefore, you need to find space, power and places to host it all. It is no mean feat. This Bill potentially could look at all of us having almost to mirror our entire network's traffic to enable us to filter it. It is a huge undertaking.

Mark Hughes: You asked about costs. We believe quite strongly that the costs should be met by the Home Office—that we should seek to have 100% of our costs in this space reimbursed. The reason is that, if you start from the basis that there is no cap on the cost, you may end up with a disproportionate technical solution that could be overintrusive, so the cost in itself will help bound the solutions.

Mr David Hanson: To help the laymen and women among us, if the taxpayer chose to support the cost of developing this scheme, do you think £170 million is a reasonable estimate, given what you have said in your previous answers, or not?

Mark Hughes: Based upon the assumptions we have seen, from our point of view, yes, because it would cover what we need to do, but if you aggregate it across the industry—

Mr David Hanson: It is not just you, is it?

Mark Hughes: Absolutely not.

Mr David Hanson: Otherwise the terrorists and criminals would not use BT; they would be using something else, would they not? So it cannot just be you.

Mark Hughes: Indeed. There are obviously other ways in which other networks are architected. There are, though, other assumptions. You could use less sampling of traffic, which would perhaps give less coverage, but there would be a trade-off in the amount of cost.

Q107 **Mr David Hanson:** This is the final question from me, Lord Chairman. Let us look two or three years ahead to when this has all been done, someone has paid for it, it is all available and the aspirations on page 25—of the Government and you—have been met. What do you think about how the Government access that material? Are there sufficient safeguards in the Bill for single point of contact officers? Are there sufficient safeguards in the Bill for access by the security and police forces via the Home Secretary, or whoever, in the Bill?

Mark Hughes: On that point, the Bill is clear that there are three purposes under which the data we are talking about, the Internet connection records, can be disclosed. That is fine. However, there are further parts of the Bill that refer to forward-looking capability. We believe, going back to one of the points I made earlier, that that potentially changes the intrusiveness before the data are disclosed and would, in our view, require a check against the level of intrusiveness that it would incur and a referral back to the legal oversight to ensure that we were not stepping outside the intention that was originally conceived in the three purposes.

Hugh Woolford: Can I raise an item on the emergency single point of contact? One of the items that is suggested is emergency SPOCs. We feel that could give rise to an ability to breach the system. In an hour of need—the golden hour—how are you going to validate who is asking for the information? It would be better if the normal SPOCs—if "normal" is the right word—were to provide cover so that there was a single list of authorised people who can ask for it. Having an emergency, somebody ringing up or contacting and saying, "We need this because someone's life is in danger", gives an opportunity for that to be abused. We feel it is better if the SPOCs cover each other. That is an area that we would like to have looked at.

Mr David Hanson: Apart from that, it is all going well.

Q108 **Stuart C McDonald:** I have one short supplementary on these points. One or two witnesses made reference to a similar scheme that was operated in Denmark. Is that something you guys have looked at? What were the similarities and differences? Is there anything that can be learnt from what happened there?

Hugh Woolford: No, I have not looked at that, I am afraid.

Mark Hughes: I understand that the system in Denmark has failed because the software has not worked. That is what I am led to believe.

Stuart C McDonald: Is there anything we can learn from that? Is the scheme that you are being asked to implement similar?

Mark Hughes: I am not familiar with the ins and outs of the detail of it; I am just aware of the headline. Through the consultation and the technical feasibility that we have done, we believe there are technical solutions that we can put in place—subject to the Technical Advisory Board confirming that. They would perhaps draw on that Danish experience, but we have to be careful that we implement them properly. There is no reason why, if we have the right solution and we implement it properly, it will not work.

Q109 Lord Butler of Brockwell: I have one supplementary. Could you break down the £174 million between the one-off cost of getting the right equipment and then the recurrent cost of maintaining it?

Mark Hughes: The capital investment—the deep packet inspection-type equipment that needs to be put in place—has to be factored against the very strong growth, or fast growth, in bandwidth over the period. The Home Office looked at this over 10 years. Then there is obviously the ongoing cost of maintenance, but also primarily storage. There is an initial upfront investment, but storage is the thing that is going to take up a fairly big chunk of that cost.

Lord Butler of Brockwell: Can you give us an indication of how much of the figure you gave is the once-and-for-all cost?

Mark Hughes: I do not have the figures off the top of my head, but it is skewed quite heavily towards making sure that there is storage. It is not to say that the initial investment is not insignificant, but the storage is also a significant part of it.

Lord Butler of Brockwell: We are talking about £174 million per year, are we?

Mark Hughes: No. From my own point of view—BT's point of view—it is a fraction, so to speak, of that, but we look at it over a time period. There is an initial upfront investment and thereafter the storage.

Adam Kinsley: It is possibly worth adding that, whereas in the previous regime data growth did not matter that much, in this regime it very much would and data growth is running at doubling every 18 months or so. That needs to be factored into any equation.

Q110 Suella Fernandes: It will be a challenge to maintain the security, but to assess the challenge that is going to be presented by the Bill, what in a technical capacity is available to you to reassure the public on the security of data retention?

Hugh Woolford: We have discussed this. We will obviously look to work with the government security advisers to ensure that any processes and systems that we put in place to meet this Bill would meet those requirements and then regular auditing of them. That is the best way we think we could assure that everything was secure and in place. As a matter of course, you have to create a culture and a process around it that brings rigour.

Suella Fernandes: What is your assessment of the effectiveness of things like firewalls and personal vetting systems, and how realistic are they as tools to expand on?

Mark Hughes: It is about creating a layered approach to defence, ensuring that the controls are proportionate, given the sensitivity of the data. We are talking about collecting data for the first time—data we have not collected before—and the key is to ensure that our customers and their rights are protected. That data has to be looked after very carefully, so we have to have a commensurate security wrap around them that takes account of our customers' human rights and indeed their privacy as well so that we ensure that we maintain and safeguard that.

Adam Kinsley: We currently work with the Government on standards, but it could benefit from being more joined up on the Government's side. The Home Office, the ICO and the National Technical Assistance Centre having a single set of standards that we could build to would make a lot of sense.

Mark Hughes: We see a key role for the proposed Investigatory Powers Commissioner and its office being responsible. Clearly the Information Commissioner's Office has a role as well, but it would be useful to us in this context to have a joint agreement between the Investigatory Powers Commissioner and the Information Commissioner's Office, perhaps through a memorandum of understanding. We would rather have the Investigatory Powers Commissioner as the authority to which we could go to seek advice to ensure that we were meeting the correct standards to safeguard that information.

Suella Fernandes: Of course the Information Commissioner will have an auditing power over the security of the systems. How would you describe the appropriate level of engagement with the Information Commissioner?

Adam Kinsley: In the past we obviously had normal business interaction with the Information Commissioner. It seems to us that with this opportunity, when we are creating a new commissioner for these purposes, it might make more sense to bring all of that under one roof; if we are looking at the security of these specific systems, now might be the time to look at having it all under the Investigatory Powers Commissioner rather than two separate organisations.

Hugh Woolford: We absolutely echo that. It brings clarity and conciseness. That is our absolute view. We would rather have it brought under one, definitely.

Q111 Suella Fernandes: This is my last question. There is some suggestion of introducing a criminal offence for data breach by communication service providers. Do you think that is going too far? Do you think it could act as an incentive?

Mark Hughes: We take the privacy and security of our customers' data extremely seriously. As is well reported in many parts of the press, it is something that we take so seriously that we do not necessarily see criminal powers as necessary. We already take it extremely seriously and we believe that the sanction if something goes wrong is that one can quite clearly see the consequences almost on a daily basis.

Hugh Woolford: That is more or less what I was going to say.

Q112 Stuart C McDonald: I want to ask about request filters. What is your understanding of how a request filter would work, and what concerns, if any, do you have regarding its operation?

Hugh Woolford: We have had engagement on the request filter. It is not specified as such in the draft of the Bill. We understand that information would be asked for, we would pass it into a filter and then ensure that only the specific information is passed back, so it stops massive information coming back. We have a few specifics, but the principle is purely at high level, as a concept more than anything else, at the moment. Without wishing to sound like a broken record, this is something else that definitely needs to be looked at and worked through in more detail. One thing that we do not want to do is to become data analysers of information.

Mark Hughes: We understand that it is for the Home Office to design and build the request filter and that it will sit between us as a communication service provider and the law enforcement agency. That is how we see that it will work, but, as Hugh said, there is more to be done. It will use an algorithm essentially to limit the data that are disclosed or presented to the law enforcement officer, who is obviously authorised to see the data, so it limits the data just to those who are necessary to that question.

Stuart C McDonald: Does the information you have just given arise from discussions you have had with the Home Office?

Mark Hughes: It is what I understand from discussions we have had with the Home Office. We have a concern, once the system is effective and in place, that there could be a situation where lots of questions are asked and continue to be asked of it, so our view is that more work needs to be done through consultation to ensure that we—again, going back to my previous point about intrusiveness—level up if multiple questions lead to a point where it is becoming overintrusive. An important principle for us throughout the Bill is that we should always level up to the highest level of authority when we think intrusiveness is becoming greater than was originally intended.

Lord Strasburger: There is a view abroad that the provision in the draft Bill for the request filter is not much more than a placeholder for the Home Office to return to this in the fullness of time and, effectively, write its own cheque on what this will deliver. From what you are saying, it is not giving you very much detail about what this is to do. Is that a possibility?

Adam Kinsley: I would not like to comment on whether it is a possibility. As I understand it, the request filter is there to limit and to be a protection against the flows of information. I would not want to speculate where it might go. We certainly have not seen—

Lord Strasburger: The fact is we do not know where it is going.

Adam Kinsley: The fact is we have read factsheets and had discussions about the concept.

Mark Hughes: The thrust of it is that it is about limiting the amount of data that will ultimately be disclosed to answer a particular question, which is important from a proportionality point of view.

Q113 Lord Henley: Can I turn to the maintenance of technical capability and what is proposed in Clause 189 of the Bill, which you will be aware of? As you know, the Secretary of State will be able to impose various obligations on relevant operators and that will take the form of a technical capability notice, and she will obviously have to consult about that. What are your views on the ability of the Secretary of State to impose a technical capability notice? How do you think your customers are going to react if they are aware that the power exists but they will not be aware of any specific imposition, because that will not be disclosed?

Mark Hughes: There are a few points on technical capability notices. The first one is that we believe quite strongly that the Bill should be clearer in its definition of the fact that the capability notice should be limited to public telecommunications services. At the moment, the definition is not clear, and we are quite clear that it should not extend to private services; it should be limited specifically to public telecommunications services. The second point is that the notice should be served on the provider who is closest to where the information can be provided from. You used the example of Facebook earlier on. That is a matter for Facebook to deal with and the technical capability notice should be directed at that organisation, if indeed it is the closest to the information, which is its information. It should be served, therefore, on those closest to the place where the information is maintained. Beyond that, the existence of a technical capability notice, as in the draft Bill, formulated through the Technical Advisory Board, is good. That there is consultation and oversight that needs to happen before it can be issued is a positive thing.

Lord Henley: What about the views of your customers?

Hugh Woolford: It is definitely not my place to comment on what the views of our customers may or may not be, I am afraid. We are concerned about that, absolutely, but at the moment we have not consulted with them or asked them, so it is wrong for me to offer up an opinion.

Mark Hughes: It is not the technical capability notice per se; in entirety, all the notices that come from this, those beyond the technical capability notices, are something that our customers need to be aware of. Transparency is one of the reasons for this new Bill.

Q114 Lord Henley: You mentioned oversight and the importance of that, and it was partly dealt with in earlier questions from Ms Fernandes about the Information Commissioner. I forget who answered this and whether it is your collective view, but I got the impression that you would like the proposed Investigatory Powers Commissioner and the Information Commissioner to be one—to be merged.

Hugh Woolford: Yes.

Mark Hughes: I am not advocating a merger, but for the purposes of the Bill we feel that for the Investigatory Powers Commissioner there should perhaps be some memorandum of understanding with the Information Commissioner. As I understand it, the Information Commissioner has many other jobs to do beyond this. There is no merging of the two, but just for the purposes of this Bill it would be useful to have one place to go to. We are all agreed that it is the Investigatory Powers Commissioner.

Lord Henley: Because the Information Commissioner is doing other things, in other words, he would delegate his bit of it.

Adam Kinsley: I am not sure how you would bring it into effect. If what we are talking about is security oversight of systems designed to fulfil the obligations in the Bill, it seems that the specialist commissioner would be best placed to carry out that function.

Mark Hughes: Can I make one more point about the technical capability notice? Following on from the point about those providing the service, and that the one closest to the service should be the focus of the Bill or any action that is served, it is not appropriate, we believe, for a network provider to be used as a one-stop shop. It is absolutely important that we process and manage data on behalf of our customers. Where that data is processed by another organisation, it should be subject to the technical capability notices.

Hugh Woolford: Adding to that, if I may, the retention and storage of third-party data is something we are also concerned about, linked with that whole piece. We do not want to be seen as that one-stop shop and asked to retain and store data for third parties that are not to do with our core business or core customer groups.

Lord Strasburger: How do you feel about GCHQ engaging in covert bulk network interference against your networks?

Adam Kinsley: I personally do not have a view on that. That is a matter for you guys to consider.

Q115 **Lord Strasburger:** My question is: how do you feel about your networks being amended covertly by GCHQ and the risks associated with that?

Mark Hughes: It is important to note that any power in the Bill that is instigated in that particular arena has to be proportionate and has to have the right checks and balances over the amount of intrusiveness. The oversight has to take account of the fact that, by their very nature, those types of powers are quite intrusive, so the levelling-up process of the oversight needs to be such that there is full legal oversight.

Lord Strasburger: My question was about the risk to your networks. That is what I was asking about.

Mark Hughes: We are certainly not in favour of anything that would undermine the integrity of our networks.

The Chairman: Gentlemen, we are very grateful to all three of you. Thank you very much for coming along and giving evidence to us.

Mark Hughes, Vodafone (QQ 145-161)

Evidence heard in public Questions 145-161

Oral Evidence

Taken before the Joint Committee

on Monday 14 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Stuart C McDonald MP, Matt Warman MP, Baroness Browning , Lord Butler of Brockwell, Bishop of Chester, Lord Henley, and Lord Strasburger.

Witness: **Mark Hughes**, Vodafone, gave evidence.

Q145 The Chairman: A very warm welcome to all four of you. As I explained to our colleagues who came in earlier this afternoon, this is a hugely important Bill. We are very grateful to you all for coming along so that we can ask for your views about it and you can put any points to us that you wish. I am going to kick off by asking all of you how extensively the Home Office has engaged with you with respect to this Bill.

Mark Hughes: It is fair to say that Vodafone has had a number of meetings with the Home Office over an extended period. The engagement has definitely been better this time than it was in the previous Communications Data Bill period. It is also fair to say that we still have concerns over a number of aspects of the Bill, so we hope to be able to talk some of those through today.

The Chairman: Generally speaking, you are satisfied with the engagement.

Mark Hughes: Yes.

Simon Miller: Before I answer the question directly, it is probably worth emphasising how importantly we regard all our customers' data security, both in terms of keeping it safe from attack and in terms of how we process it to provide the service and experience our customers want and need, which is done strictly in accordance with law. The levels of engagement have broadly been good. They have certainly been far more extensive than anything we had experienced before from the Home Office and certainly much better than for DRIPA. The engagement has taken a number of forms—and I hope I am not speaking for everyone else here—including large roundtables with the Home Secretary, timetabled sessions and informal bilateral and multilateral meetings.

The one area that has been lacking is tripartite discussions between us as communications service providers and law enforcement agencies, together with the Home Office. It is also true to say that, although the level of engagement has been good, the iterative approach to consultation has revealed a significant number of issues with the legislative proposal that the Home Office has yet to address or has not addressed. These will be fleshed out, I am certain, in the course of this session.

The Chairman: I am sure you are right.

Jonathan Grayling: To echo that, engagement has been positive and significantly better than the Communications Data Bill. There have been some regular timetabled sessions. They have been cross-stakeholder, involving law enforcement, industry and the Home Office. That has been really useful, because it has assisted in providing a common understanding of operational requirements, technical capabilities and policy drafting. That said, this is a piece of government legislation and it is ultimately Parliament's decision what is and what is not included in the Bill. EE's main priority is our customers' privacy, and as such there are still a number of areas in the Bill that we have some concerns about, which we hope we can bring out in the next hour or so.

Adrian Gorham: I will not repeat the comments my colleagues have made, but it is certainly much better than we have seen in previous legislation that has gone through, so we are very pleased about that. We have had a good level of debate.

The Chairman: That is an interesting start.

Q146 **Lord Henley**: It is very pleasing to hear that the Home Office has been consulting, speaking as one of the various former Home Office Ministers on this Committee. We understand there is a shortage of IP addresses, and we also understand you do not always record which subscriber had which IP address and which port number at any specific time. What can you tell us about the practical difficulties and the costs that might be incurred in conducting IP resolution?

Adrian Gorham: When they developed the IPv4 standard, there were 4.3 million addresses worldwide, so that clearly was not enough, as technology took off, to give each customer an individual IP address. When the mobile phone business moved into doing internet connections, we had to come up with a solution to that, because we could not give every customer their own unique IP address. They developed a technology called network address translation, which means that every time you go on to the internet and have a data session, you are given an IP address, for a very short period, for that transaction, and then it just drops off. The next time you do something, you are allocated another one, so it is very dynamic and it changes all the time.

We had no reason to make a record of that. That is our challenge. We now need to record what number we allocate to each session and store it, and build the devices so that we can disclose that to the authorities.

Jonathan Grayling: To pick up on Mr Gorham's comments, the key point here is that at the moment the technology does not exist to be able to resolve that IP address. The public-facing IP address could have multiple thousands of unique devices attached to it. Indeed, trying to resolve that public-facing IP address to at least a near one-to-one match—and that is Parliament's intention—will require the retention of internet connection records.

As I said, the technology does not exist at the moment. We are in the feasibility stage now. At the end of that feasibility stage, it will probably take up to 18 months to deliver a solution because of the complexity involved.

Simon Miller: There is not much to add to that, other than to say that the technical challenges faced by my colleagues at both O2 and EE are replicated across the board.

Mark Hughes: I have just one thing to add. Vodafone is in exactly the same boat. We do not keep the IP data of all our customers. We are going to have to deploy new technology to be able to do this. The other thing that has not been said so far is that we will need a very big storage system to be able to keep it. It is a significant amount of storage.

Q147 Lord Butler of Brockwell: Could I take a step back and ask about the existing system and the requests you get for call data records under Sections 21 and 22 of RIPA? We know that is a diminishing resource as far as the intelligence agencies and law agencies are concerned, but are you satisfied that, to the extent you still have those records, that system works reasonably well?

Jonathan Grayling: Yes, the current acquisition arrangements under RIPA work well. One of the primary provisions, which is tried and tested, is the SPOC system. Essentially, that is the provision of comms data to law enforcement and the SIAs to a single point of contact. The use of SPOCs provides a strong, transparent and stringent process. As I said, it has been tried and tested over many years. Their SPOCs are specially trained. They are accredited in the use of CD, so they can advise their respective officers within law enforcement and the SIAs on what CD needs to be acquired.

That said, we also welcome the additional safeguards in the Bill. We welcome the requirement for a designated person, independent from the requesting agency; the streamlining of existing legislation and repeal of old legislation, so the Investigatory Powers Bill will be the primary piece of legislation for the disclosure of CD; and the restriction of ICRs to certain authorities and for certain purposes. Moving into the IP world, keeping the SPOC community and law enforcement up to speed with new technology is going to be a challenge, and a significant amount of effort will be involved in ensuring that law enforcement and SPOCs can interpret the data that we are talking about today.

Lord Butler of Brockwell: Going forward, then, into the new world—you have begun to describe the complexity to us—is it practicable, by using the internet connection records, to distinguish just the first line of the address, which is what the Government want to do, and to draw a line between that and what would be more revealing about the content?

Mark Hughes: This is where we get into some of the more technically challenging areas of the Bill, for sure. It is important that we call this out as it is. We are talking here about web browsing data when we talk about internet connection records, so we need to recognise that this is a hugely sensitive part of the capability that is looking to be developed. In terms of how easy it is, this is where we start needing to talk about over-the-top or third-party service providers, who may be running their communication services under the underlying network providers that are here today.

To try to bring this alive with an example, Vodafone and everyone else here will act very much like a postman today. We would carry a packet of data, or a letter in this scenario,

from point A to point B at an IP address. We do not know what is contained in the letter in this scenario. In future, the challenge for us is having to open that letter. Let us say it is a Skype service. We would have to say, "Okay, now we have opened it, we understand that a Skype service is being provided", and the Skype username or ID of the person would be within that. You can already start to see how the lines are being blurred between traffic data and content when you start having to open packets of data as they cross the internet.

One of the main concerns here, especially around third-party data, is that, today, Vodafone has no day-to-day business use for this data. We do not create it, so we are going to have to generate new data about our customers that we do not generate today. Secondly, we do not understand its structure. That structure can change on a day-to-day basis, and it is encrypted, so we will have to be able to strip off the electronic protection and decrypt it before we can store it. We would be concerned about attesting to the accuracy of that information as well. I am also concerned about possibly creating a single point of cyber vulnerability when you start decrypting things to be able to store them. There is a very good reason why they are encrypted in the first place. I am concerned that we will perhaps solve one problem, but not necessarily in the best way, and create another cybersecurity problem. Our point is that the very best people to keep data about the services being provided are the third parties. They should be the people who are keeping information to help law enforcement fight crime in this country, rather than the underlying service providers.

Lord Butler of Brockwell: Give me an example of what you mean by the third parties.

Mark Hughes: I gave you an example there. It could be a Skype; it could be WhatsApp. It is those types of service providers.

Lord Butler of Brockwell: I see, so the people for whom you are carrying the traffic. Okay. You have talked about this being a very complicated process. Can you give us some idea of the costs?

Mark Hughes: Until we have been served with a notice, I would be purely speculating as to the cost. I would be uncomfortable giving you any kind of idea until the Home Office has served us with a notice. It would be significant, it is fair to say.

Lord Butler of Brockwell: The Home Office produced a figure, if I remember correctly, of about £180 million. Do you think that is an overestimate or an underestimate?

Mark Hughes: Where this figure from the Home Office came from I cannot say, because we were not consulted when it was put together. We were consulted only after that figure was put together. I would not be able to speculate, from a Vodafone perspective, as to how much it would cost.

The Chairman: Would all four of you agree that the cost implications are considerable, significant, huge, something you can manage, or you do not know at this stage?

Adrian Gorham: It is going to be huge. Also, there is the way data is exploding. The increase in data is about 100% per year. That is the big issue with costs; this is going to double by

next year, with the way the internet is going. There are going to be big increases in the future, with huge amounts of data.

Jonathan Grayling: I agree. Going back to what Mr Hughes and Vodafone said, unless we can be explicit in the Bill about exactly what data we are going to be required to retain in any future data retention notices, it is simply not possible to give a figure. If there is, within the legislation, scope that third-party data falls into our areas of responsibility, the costs will be even more. We are only focusing on the data that we understand now, the data that traverses our network, the data that we require in order to route a communication and provide a service to our customers. Even then, it is incredibly difficult to come up with a cost.

Q148 Lord Butler of Brockwell: I have one final question. I get the impression that you are not enthusiastic about this provision in the legislation. You think it is a lot of work. Even if the Government meet the costs for you, you are not enthusiastic participants.

Mark Hughes: It is not necessarily about being enthusiastic. We absolutely recognise the challenge that law enforcement and Government have here. Vodafone's concerns are very much about making sure that we have a Bill that is technically workable. At the moment we are really concerned about being able to keep data about a service that is nothing to do with our core business, generating new data about our customers and especially stripping off electronic protection and decrypting communications passing through the internet. This is a highly challenging arena for any of the companies here today in which to do things on behalf of somebody else's communications services. We feel that the third parties providing those services have an obligation here to assist law enforcement fight crime.

Q149 Bishop of Chester: Clause 193 gives a series of definitions in the Bill. One of the issues we have been wrestling with is the distinction between data and content. That is in subsection (6). Are you comfortable with that distinction between data and content in the context you are describing?

Jonathan Grayling: This is an incredibly complex area and, with respect to the Home Office, it is even more complex to try to define within a piece of legislation. Without wishing to go over the ground we have just covered, there are issues in relation to what is perceived as content and what is perceived as CD with respect to who owns that data. The definitions provide a basis for further discussion. It is a starting point, and it is a starting point for defining those capabilities. That said, echoing what we have just spoken about, to a CSP, to a network provider, the communications data is the data that is available to us that we see in order to provide a service to our customers. Essentially, that is the data we need in order to route a communication that we will process and that we will make a decision on. If we do not make a decision on that data, we do not perceive that as being our data. It is simply data attached to a packet, but the data within a packet could be communications data to the sender of that packet.

Again, if you talk about WhatsApp, all we are interested in doing is sending the WhatsApp message that traverses our network to the WhatsApp server. If you were to open that WhatsApp message, you might find out to whom that message was being sent, but we have no need to know that; we are just sending it to the WhatsApp server. That data could, to WhatsApp, be perceived as communications data, but, because we have to open the

packet, it is content to us. This is where there are blurred lines and why we are looking for clarity in the Bill as to exactly what data we should be required to retain as communications service providers.

Adrian Gorham: To build on Mr Grayling's point, another issue here will be the encryption, because so much of the data now going over our networks is encrypted by those application providers. In a lot of cases, we cannot see what is contained within that traffic. They are not going to give us the keys so that we can decrypt it to examine it, so in a lot of cases we are completely blind to that traffic.

Simon Miller: The issue here is that there is a clear need for further discussion with the Home Office to arrive at a text that works. There may be a need for further interpretive text, potentially in the Bill, but there is definitely a need for more than there is currently. The introduction of the ideas in the Bill is useful, but they need further unpacking.

Bishop of Chester: Do you think your customers would make that distinction between content and data, or would they think that the data is quite personal to them, quite apart from the content?

Mark Hughes: We know that customers would expect all the companies here today to look after personal information to the highest levels possible. Concerns about decrypting third-party communications as they cross the network would be of a concern. Again, it touches on the point that the persons who should have the obligation here are the third parties. They do not need to break the encryption because they have created the communication in the first place.

Q150 **Lord Strasburger**: Putting the last two topics together, encryption and degree of difficulty, with the proportion of internet traffic that is encrypted increasing by the day, is it possible that you will end up in 18 months' time with an expensive and rather complex system to collect these internet connection records, a diminishing part of which is of any use because encryption has increased?

Jonathan Grayling: That is a real risk. Technology is moving on so quickly. New protocols, new algorithms on the internet, are being created all the time, which makes it very difficult for us to see those communications. Yes, you have encryption, but you just have the way the internet is developing in itself. I would not like to talk about timescales and I would not like to comment on the actual benefits that the technical provisions we are introducing would give to operational law enforcement and the SIAs, but it is a risk that technology is moving so quickly that we may be behind the curve.

Q151 **Baroness Browning**: The three-level categorisation of communication in the RIPA legislation has been replaced by two: entity data and events data. Do you feel that reducing these categories down to two levels causes a problem? Are they sufficiently clear and workable? Is that a good thing? Is that going to cause you problems?

Adrian Gorham: In its simplest form, it does not cause us a problem. There are going to be two types of data. There will be entity data, which is about the actual person; it will be your name, your address, your telephone number, so it is about the individual. Then there will be the events data, which describes the event and will be about where something took place, the location. The good thing about those two fields is that a different level of

authority is needed by the police if they want that data. If it is about you as an individual, that will be authorised by an inspector, and if it is the broader data that includes the location, that will be signed off by a superintendent. That gives us clarity about what is required. The challenge is that as we move forward and more and more communications are coming online and more and more machine-to-machine, there will be different fields of data and we will have to have regular discussions to find out where those fields sit.

Mark Hughes: We were clear about the previous definitions. We are not clear why it needed to change, but we have no particular objections to the proposed changes.

Baroness Browning: With the advance in technology, are you referring to the fact that things that are not in use now but are coming up over the hill are things you will have to take decisions on?

Adrian Gorham: In the future, you are going to have SIMs in your fridge and your dishwasher. All these appliances are going to have SIMs in them that provide data. That all has to go into this process, and we are going to have to make those decisions where things sit.

Q152 Mr David Hanson: It is important in this session to try to nail down in some detail what you believe the Government are trying to do and whether you can deliver it. Could you just indicate to the Committee your understanding of internet connection records, as of the Bill's description?

Mark Hughes: It goes back to what I was talking about earlier. Internet connection records are web-browsing data, so they are not the page you end up landing on but the domain that you have visited. They do not exist today, so this is about us having to create and generate entirely new data sets.

Mr David Hanson: For Vodafone, how easy is it to deliver that new data set as of today?

Mark Hughes: It is extremely difficult, because, as we have heard, the vast majority of over-the-top service provider data that would be an internet connection record is encrypted and it is not data that we understand or in a structure that we have any understanding of, because we have not created it. We are now going to have to create an entirely new type of data on behalf of another company, decrypt it and then store it ready to disclose potentially in a court of law, where we cannot even attest to the accuracy of that information. It is very difficult.

Mr David Hanson: Vodafone is an international company. What demands are being made on you by other nations outside the UK in this field at the moment?

Mark Hughes: There is no standard approach internationally. There is a real patchwork, depending on the country. There is no one model. The UK model is certainly the most transparent, but there is no one model that fits all.

Mr David Hanson: What is other colleagues' understanding of what an internet connection is?

Adrian Gorham: This still has to be clearly defined.

Mr David Hanson: The Bill is in front of us now. Is it clearly defined for you in the Bill?

Adrian Gorham: We are nearly there on the clarification of what makes up the record. The challenge is that this is something we have never kept previously. We keep your CDR for every phone call you make. We keep the record, we store it for a year, and we can disclose it. This is a completely new kind of record that we are going to be keeping, and then we have to hold it, store it and disclose it, so it is a big step up for us in what we need to do and provide.

Simon Miller: The issue here is that we know that an internet connection record is going to be something like a simplified version of a browser history, but we do not know exactly what it is going to be. Until that bit is nailed down, we cannot ascribe a cost to it or know exactly how difficult it will be to implement. We do know that it is going to stretch our existing capability many times.

Jonathan Grayling: The key point here is that an internet connection record does not currently exist and we have to create it. Even once created, it may not exist as one whole record. As Mr Gorham said, we are beginning to get some clarity on what the Home Office believes an internet connection record may be made up of, the subsets of that internet connection record. Some of that data may or may not be retained. The issue is putting it all together to try to create something that is going to be of use.

Mr David Hanson: We are the draft Bill Committee. The real Bill Committee will meet in the Commons and the Lords, probably from the end of February until the end of July, and then this will be law. The question to all of you is: are you satisfied that, by the procedure of considering this in both Houses of Parliament, the definition, the deliverability and the apportionment of cost will have received sufficient attention to have confidence among your companies and the public that it is being done to the standard the Government expect?

Mark Hughes: Until the Home Office serves us with a notice as to exactly what it wants, it is difficult to speculate. We all understand it to be web browsing; we know that it is going to be difficult and challenging and that it will create lots of new data, which is going to be highly intrusive, but until we have a notice and know exactly what we have to keep about which companies, it is difficult to speculate.

Simon Miller: There has been a process of engagement in place that has got us this far and has led to improvements in what is being proposed. That suggests that it is possible to get this over the line. However, there are still a substantive number of challenges that need to be met in order to do that. At the moment, we have not necessarily had the responses from the Home Office that we either want or need on this in order to have full faith in that process.

Mr David Hanson: Is that the general view?

Jonathan Grayling: You cannot underestimate the complexity.

Mr David Hanson: Well, let us just go back to the point that Lord Butler made earlier about the costs, again, which the Government have estimated at approximately £170 million to £180 million. We had a panel in front of us last week in another Committee room who

basically said that they estimated that they had spent £170 million, just among the two to three companies in front of us that day. Again, it is important that you, either now or before the Bill reaches deliberation stage, as well as negotiating with the Home Office, are clear about the implications in relation to the costs. The Houses of Parliament cannot pass legislation that will not be deliverable, and it is going to have burdensome costs, on the taxpayer, the public, or both. Can you give the Committee any estimate now? Could you tell the Committee, "We think it is in the ballpark figure of X"?

Mark Hughes: Again, without wishing to be evasive on this question, it depends on how much of the internet traffic the Home Office wants us to keep. Is it every single third-party service? How quickly do they want it decrypted? How much of it needs to be stored? Is it for the full 12 months, like everything else? How much resilience does it need? Do we need one set of resilience, or do we need to be able to build it three times just to make sure that it goes down? Is it that important? It is those sorts of factors that can make this change from one number to something completely different at the other end. The only thing I can say, given what we know is in the Bill and what we know about the technology in this area, is that it will be a significant cost. Saying how much it will be would be me picking an item out of the air and literally speculating. It is going to be significant.

Mr David Hanson: I take it, by the looks of agreement and nods, that that is pretty much where the panellists are. Could I just then throw the other question in, which is still an important question? Ultimately, whatever the cost is fixed at—and you have said there will be a cost—who, in your view, is responsible for the apportionment of that cost? Is it something you take as a commercial issue? Is it something the Government have to fund 100%? Where do you land on that figure?

Jonathan Grayling: We believe that the Bill should make it explicit that a company impacted by this legislation is fully able to recover the costs incurred. We believe that if there is no cap on costs based on a proportionality aspect, and the obligation and the financial impact is simply passed on to the CSP, this could result in delivering disproportionate solutions. If there is a cost recovery model that places a cap on cost and is based upon proportionality, that provides a far safer investment for taxpayers' money and the privacy of our customers.

Q153 **Mr David Hanson:** Is there any disagreement with that? No. I have one final set of questions. Ultimately, if it is doable, if it is defined, if it is delivered, and if it costs something, at some point a police officer or agency is going to ask you for information. Are you satisfied that the Bill has sufficient provision in relation to the single point of contact from officers? Is that sufficient to give your customers and you the security you believe you would need?

Jonathan Grayling: It goes back to the point that until we know exactly what data we are required to retain and the format that it is going to be stored in, it is impossible for us to say whether a SPOC or a police officer is going to be able to interpret that data, because that data does not exist at the moment. That record simply does not exist, so we cannot say whether a SPOC community is going to be able to interpret, because we do not know what they are going to be able to interpret yet.

Mark Hughes: It is fair to say that the SPOC community will have to undergo an extensive amount of retraining to be able to understand this and make use of it in a day-to-day

investigation, especially considering how quickly, sometimes, they have to be able to make a decision based on this data in grave situations.

Mr David Hanson: I will come back to the final point: this could be law, in one form or another, by September 2016. What is your assessment of the deliverability, as of today, of the Bill as it stands?

Adrian Gorham: We would all accept that this is a big step up in capability. Everybody understands the challenge that the police and the security agencies have, and we all understand the capability gap they have with modern communications. This is going to be a step change for us, and that is why the discussions we are having with the Home Office are quite detailed, because we need to get this right. I am sure that everybody else on this panel, as well as me, wants to make this work and to ensure that taxpayers get good value for money. The only way we can do that is by having the strong discussions now, so we are very clear on what we need to provide and we do that in the most cost-effective way.

Mark Hughes: Regarding deliverability, without wishing to keep harping on about the same point, the easiest and most elegant way to deliver this capability is for over-the-top service providers to have the same obligations as companies here do today to assist law enforcement with information about customers who are using their services who may be breaking the law.

Q154 Lord Strasburger: On the subject of deliverability, Mr Hughes, you have twice said, "Then we will have to decrypt the data". How can you possibly do that unless you get co-operation from over-the-top providers, such as Facebook and others, or you get sufficient information from them as to how to decrypt that data, or from end users regarding how to decrypt their data? How can you do this?

Mark Hughes: You are absolutely right. The point of this is that we will have to be supplied with new technology, from law enforcement or intelligence agencies, to be able to decrypt that information about third parties and store it. That goes back to the point, again, that it is not preferable for our companies—certainly not for Vodafone—to be able to decrypt communications and store this. It would be much more elegant for the third-party service providers to have this obligation to assist law enforcement to fight crime.

Lord Strasburger: Presumably, by treaty, bearing in mind that most of them are American.

Mark Hughes: The Bill itself allows the Home Secretary to place an obligation on any person. Most, if not all, providers—certainly the big ones—have infrastructure and offices here. Given the way the internet is structured, there are things globally; I see no reason why the third parties would not want to assist with helping law enforcement in this space.

Stuart C McDonald: Mr Hughes, I think you said that you would not be able to attest to the accuracy of ICRs. Is that because of this process of decryption, or are there other reasons why you would not be able to do so?

Mark Hughes: It is fair to say that if we were able to extract data belonging to another provider, not understanding its structure as it crosses our network, I would be

uncomfortable with being able to explain the accuracy of another company's data. That would be an incredibly difficult thing for Vodafone to do.

Stuart C McDonald: So you might not be able to come up with accurate ICRs at all.

Mark Hughes: An ICR does not exist today. Once it is created and we have solved all the technical challenges that we have already discussed, I would imagine that it would be tested in court once this evidence becomes as bread-and-butter to the criminal justice system as mobile phone evidence is. I would imagine that it will be tested very heavily on the grounds of, "Who created it? How did you decrypt it? How accurate is it? If you did not create it, how can you attest to the accuracy of it?" Companies here, such as Vodafone, have to attend court to be cross-examined on mobile phone evidence that has been collected. We would find it extremely awkward to have to attest to the accuracy of data that we had not created in the first place.

Suella Fernandes: You appreciate, do you not, that the current lack in capability—for example, the requirement to keep internet connection records, or store them—means that the agencies can paint only a fragmented picture of a known suspect?

Mark Hughes: I absolutely recognise that.

Q155 **Suella Fernandes**: Examples abound, but in a recent referral of 6,000 profiles from the Child Exploitation and Online Protection command to the NCA, around 800 of those could not be progressed because of the lack of this capability. That is about 800 suspected paedophiles who were involved in the distribution of indecent images whose details cannot be gathered by the agencies. Bearing in mind the benefit that is gained by this storage and retention requirement, what alternatives do you think are viable while providing a similar benefit?

Jonathan Grayling: We are not necessarily questioning that there is an operational case for this. We work closely with the NCA; we work closely with CEOP. We are just trying to reflect the technical complexity involved in meeting the demands of law enforcement. We all have a duty of care as operators; we want to be good corporate citizens as well, but if the technical complexities are there, those are the facts, and we are trying to work through those with the Home Office to provide the provision that they are looking for.

The point that you raise there about CEOP goes back to the point about the knowledge of the law enforcement community. Certainly, the NCA are pretty advanced through the CEOP side of things in relation to trying to highlight these gaps in technology, and we work very closely with them on trying to close those gaps, but it is proving very, very difficult. The technology just does not exist at the moment.

Mark Hughes: I absolutely recognise what you are saying. We care passionately about assisting law enforcement. We take extremely seriously all the obligations that are placed upon us, and we do everything we can to give the best service to law enforcement through the system, with the things that we are obligated to do by law. As Mr Grayling has just said, we want to make sure that when this legislation passes and it has gone through the correct level of scrutiny, the obligations are technically workable and we can continue to provide the level of service that the police and law enforcement agencies expect from us. We get

how important this stuff is, and we really want to make sure that we can provide the data in the best way. Again, so much of this is going to be about over-the-top service providers that we must make sure it is achieved in the simplest way possible, and the simplest way possible is for those third parties to co-operate with law enforcement.

Suella Fernandes: In terms of maintaining the security of stored data, you use firewalls and personal vetting systems, and those are effective ways of keeping data secure.

Adrian Gorham: All the operators here are very experienced at looking after our customer data. We all have a layered approach; there are different systems and processes for keeping it secure. All this means is that we are going to have even more data that we will have to keep secure.

Interestingly, one of the parts of the Bill talks about a request filter, which will be run by a third party; a third party will take bulk data from us and analyse it for the police, to make sure the police only see the data they require. My concern there would be that that third party has exactly the same level of security that we deploy ourselves in our businesses. A number of us have international standards; I would expect that third party to have that level of security, if it has my customer data. I would expect the governance that we are putting in place to go and do audits on that third party, and I would—if I am giving them my customer data—expect to be able to go and audit them myself, to ensure that they are living up to our standards as well.

We are all very used to looking after security and protecting that data, but we now, with this Bill, have a third party whom we would need to give data to, and we need to be very sure that the same level of security is deployed there as well.

Q156 **Suella Fernandes**: Lastly, retention is subject to stringent controls; it needs to be necessary, proportionate, signed off by an independent person, and it needs to be compliant with various case law and the European Convention on Human Rights. What is your assessment of that consideration of lawfulness and effectiveness, combined with the exception of whether it is reasonably practical, as a sufficient safeguard to strike the right balance?

Adrian Gorham: The safeguards in the new legislation are very good. They are much improved on where we are now, and they are much more transparent. We have to ensure that the different auditing authorities do their roles and they are done properly. If you look at the recent audits they have just started doing on the operators with the ICO, they have agreed with industry what those audits will look like and what the definition and scope is going to be. The first actual audit was done last week on O2, so hopefully we will see the results of that come back. The one thing the Bill does very well is that it polices all the transparency in audit of what everybody is doing along that whole value chain.

Q157 **Victoria Atkins**: Mr Hughes, you have used the phrase "over-the-top providers" a lot. I may be the only person wondering this, but I suspect I am not: what do you mean by that?

Mark Hughes: The over-the-top providers I have referred to are companies that are running a communication service, such as WhatsApp, Snapchat, and Skype. They are examples of over-the-top service providers; they run a communications service using the underlying network providers that are here today.

Victoria Atkins: This is what I want to focus on. You have talked about how it would be more "elegant"—I think that was the word you used—for over-the-top providers to store this information, rather than you guys; sorry for being so informal. How on earth is law enforcement to know that one of the suspects that Ms Fernandes has referred to is on WhatsApp, Facebook or whatever unless they have that link in the middle, which is where you come in, signposting them to that application?

Mark Hughes: That is an excellent point. On signposting, we would have a role to play in saying, "We need to point you towards the company where you need to go to get the rest of the information about that customer", in a way they produce it and understand it. You make a good point about having to signpost the police in the first instance to what company has produced the communications service in question.

Victoria Atkins: If we just put that into the context of your evidence, you are not saying that your companies should play no role in this; you are worried about the details of decrypting and so on, but you understand that the Bill is phrased as it is to help law enforcement link a suspect to apps or services that they cannot know about unless you are involved in the middle.

Mark Hughes: Absolutely. This is about making sure that we do not blur the lines between traffic data and content by us having to open up all the packets of the data and then provide in an evidential way all the information to law enforcement.

Mr David Hanson: It is also about shifting the cost, is it not, from your perspective?

Mark Hughes: The Home Office has always had a policy of 100% cost recovery. They have assured us that this will continue. This is not an area that we make any money out of. We provide the very best service that we can to assist law enforcement.

Adrian Gorham: Another point worth making is that the customer of this is the police officer who wants the intelligence to allow him to make that arrest. If he believes that his target is using Facebook, the target may be using Facebook but it can use it on many different bearers. So it may use the O2 network; it can then go into a Costa Coffee and use a wi-fi network; it may then go somewhere else and use BT's wi-fi. It can use many different bearers, and you have to somehow get all that data from those different companies and put that all back together to show what that individual was doing on Facebook. If you go to Facebook and they have the encryption keys, they can tell you what is going on. They have all that data for that individual, so I do believe that it gives a much better service to the police to go to that one point of contact than try to go to each of the bearers that are carrying those communications.

Q158 Stuart C McDonald: You referred earlier to the process of setting up filter arrangements to get that communications data. What is your understanding about how request filters will work under this legislation, and would you have any concerns about the operation of request filters?

Simon Miller: We understand that the request filter is a mechanism by which large amounts of bulk or collateral data provided by us as communications service providers, as a consequence of requests made by law enforcement agencies, will be gradually—through a process of correlation and different data points—narrowed down to identify either a single

subscriber or a smaller subset of users, and that this will be done by a trusted third party. The whole purpose of this request filter is to minimise the amount of unnecessary bulk data that will be handed over to law enforcement agencies.

We are all agreed as to the principle of this. There are a number of concerns, which Mr Gorham has alluded to, regarding the detail. The first is the fact that we would still continue to provide bulk data to a third party, and in so doing could be in breach of our duty of care under the Data Protection Act and the Privacy and Electronic Communications Regulations to our customers' data. The second is that we have absolutely no detail on what this trusted third party would look like, the form it would take, or the legal obligations that it would be under. As a minimum, we would simply expect that whatever operation the request filter undertook was done to the same standards, and was as secure, as our own arrangements.

Stuart C McDonald: So you have no idea who these third parties would be at all.

Simon Miller: Not yet, no.

Stuart C McDonald: What exactly is the filter? Who is responsible for putting that together, and would you have any ability to review what the filter was doing to your data?

Mark Hughes: I do not know who would be providing the service. I think it would be for the Home Office to select a vendor, to be able to build that situation. In principle, it is a good idea to be able to prevent lots of collateral intrusion. When you have really big, complex inquiries that you are running as a police officer, where you may need lots of data, the filter can be a way of reducing the collateral intrusion. The important thing here, as Mr Miller just said, is that whoever operates that has to operate it to the same standard in terms of the data that is being provided out of it, because this could fundamentally change the way network operators give evidence in court. Remember: we are potentially providing information into the filter. The operation, and what changes in the middle and what ends up on a police officer's desk from the query they have run is being provided by a person in the middle, a third party service—a vendor in this scenario. Again, we would need to make sure. It is going to take a lot of close collaboration to make sure this works well.

Stuart C McDonald: What sort of things would you want to see in the Bill so that you could have faith in that filtering process by the time you arrive in court to speak for the accuracy of the data you have provided?

Mark Hughes: We want direction and understanding on which parts of the evidential chain we would be expected to stand up in court and be cross-examined on, and whether, if the data had changed in the middle in some way, it would be the third party—for example, in this case, the vendor who is providing the service—that needed to attend court. I appreciate that these are sort of in the weeds, and they are quite technical things that we need to be thinking about, but essentially we are giving evidence in court on a day-to-day basis on mobile phone evidence, and we are worried about making sure that we can continue to do that with what is essentially a new piece of kit in the middle of the network.

Simon Miller: At the moment, this may be an issue for guidance, but these are discussions that the Home Office is yet to have with us, so we are dealing with an unknown. We are very keen that these discussions continue, and that these issues are bottomed out.

Stuart C McDonald: Any further thoughts?

Jonathan Grayling: Just to reiterate, the panel has said that the Bill places an obligation to provide security controls in relation to retained data, and those security controls are audited and will be audited. What is not in the Bill is that there are similar security controls for the request filter, and subsequently the customer data—my customer data that I am supplying to the filter. I would like to see the filter having the same security controls as the ones CSPs are compelled to provide in relation to retained data.

Q159 Matt Warman: Can you say a bit about what you understand by a technical capability notice, and what you understand by the Home Secretary being able to impose one at will?

Mark Hughes: Our understanding is that this is about the potential for equipment interference. Vodafone has three real concerns about this particular item. First, equipment interference could obligate a network operator to introduce, say, a backdoor or a way to launch some kind of attack against a particular target that may be using the network. You will probably not be surprised to hear that we have three concerns. First, we are worried about this representing a real diminution in trust in UK-based service providers, which may have to introduce backdoors on their network. In such a highly competitive marketplace, if you had to decide who to place your communication service providers with—a UK-based company that potentially has this obligation, or somebody else who does not—you may be really thinking about that.

Secondly, we are concerned about an obligation that may ask us to fundamentally reduce the level of security of our products or services, or our networks. We would be really concerned about introducing any reduction in the level of security of our products and services. Thirdly, we understand that, as it is written in the Bill, this may involve our people and our staff having to get involved in launching such attacks against targets across our network. We would be keen to make sure that that does not happen, and it is down to the law enforcement or the agencies to manage the workable provisions of that.

Matt Warman: Any other thoughts?

Jonathan Grayling: I would echo what Vodafone said there. With respect to the Bill itself, there are a number of aspects of control and oversight over those technical capability notices that we do welcome—significantly, the fact that the Home Secretary has an obligation to consult with the respective CSP prior to serving a technical capability notice on that CSP. That consultation has to take into account, among other things, proportionality, technical feasibility, the cost—which is significant for us—and the impact on our customers and our network.

Even after that consultation process, and a notice is served, there is still a mechanism whereby if the CSP is still unhappy or concerned with that notice, they can pass it back to the Home Secretary for further review and, again, the Home Secretary has an obligation then to consult with the Technical Advisory Board and the IPC, which we welcome. The key point here is that we need to ensure that each stage of that process is rigorously enforced, rather than a rubber-stamping process. If we have concerns about that, we want to have it demonstrated that the appropriate oversight and controls are being applied to that process.

Just one very quick, final point. My understanding of the Bill is that the IPC would have responsibility for the oversight of national security notices. I cannot find anything in the Bill that says that the IPC would have oversight for technical capability notices, so the question is why that might be the case.

Matt Warman: What do you think your customers would make of even an oversight arrangement that you were corporately happy with?

Jonathan Grayling: Customer trust is essential to our business, and the priority for us is to ensure that we provide a secure and resilient network. That is what our customers will expect. If there are any powers or any activity that is undertaken by the agencies in relation to equipment interference, whether that is proportionate and lawful is a matter for Parliament and the agency itself, but EE would not accept it if those activities had any impact on the security of our customers' data or the resiliency of our networks.

Q160 **Matt Warman**: Moving on to the IPC that you mentioned, do you think that the level of engagement that is outlined in the Bill between you and the IPC is sufficient to maintain that level of security and trust?

Simon Miller: The levels of engagement envisaged are broadly similar to those that we have currently with existing authorities. Interject, gentlemen, if I am talking out of turn, but those levels are appropriate to the subjects concerned. The issue for us has always been that they are broadly uncoordinated, and as a consequence of that there are business impacts. In particular, at the margins, there are jurisdictional overlaps with different authorities talking to the same subject with different voices. It therefore follows that we are fully in favour of the creation of a single body, the IPC, that will have all these powers of oversight, and it will rest in that one body. The simple fact of the matter is that the current practice of having separate bodies with these different functions is, for us, broadly cumbersome, open to misinterpretation and misunderstanding, and time-consuming.

As for the actual level of engagement, this would be a new body. We would fully expect levels of engagement to ramp up as that body beds in and to have to adapt to new personnel and new ways of working. It is probably worth saying at this point that the relationship that we all have with IOCCO is an exemplar. If the IPC were to look at the ways of working exhibited by the existing authorities, it should look to IOCCO as a model of best practice, and we would very much like to see those practices demonstrated around building strong, coherent stakeholder relations, early engagement and demonstrating sector expertise continue.

Matt Warman: Broadly, it sounds as though you are looking forward to the changes that are coming, rather than dreading them.

Simon Miller: Absolutely.

Adrian Gorham: It might also be useful if there is an express right for the operators whereby if we have an issue or a complaint about one of the LEAs or the police we can go directly to the IPC to report that. That is not to say that there have been any issues previously with them, but it is worth having in the legislation so that we have that channel should we want to use it in the future.

Q161 **Lord Strasburger**: Would you agree that equipment interference is one of the most technically complex and risky activities that we are looking at in this Bill, and do you think there is a case for having some sort of technical oversight as to what you are being asked to do from a third party, as well as having judicial oversight?

Jonathan Grayling: In the Bill, there is a mechanism to refer to the Technical Advisory Board, and we would expect that Technical Advisory Board to provide that independent oversight. Because of the additional obligations in the Bill, there should be a review of the TAB to ensure that it is structured appropriately and has the appropriate individuals around the table with the appropriate knowledge. That is necessary.

Lord Strasburger: These are very specific skills, are they not?

Jonathan Grayling: They are.

The Chairman: Thank you very much indeed. We have now come to the end of the formal session.

Sir Mark Waller, Intelligence Services Commissioner (QQ 39-46)

Evidence heard in public Questions 39-46

Oral Evidence

Taken before the Joint Committee

on Wednesday 2 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Stuart C McDonald MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Bishop of Chester, Lord Hart of Chilton, Lord Henley, Lord Strasburger.

Witness: **Sir Mark Waller**, Intelligence Services Commissioner, gave evidence.

Q39 **The Chairman:** Sir Mark, a very warm welcome to you. We are very grateful for you coming along to talk to us about this extremely important Bill and the changes it makes to the oversight of our services. Have you anything you would like to say before we open up our deliberations, or shall we go straight to the questions?

Sir Mark Waller: I wondered whether I could, in a minute, say things you already possibly know, but just, as it were, set the scene. As you know, I am the Intelligence Services Commissioner and have been for nearly five years. My primary role is to check, after the event, that the agencies have been obtaining warrants and authorisations to carry out some of the most intrusive activities that they do, and that they do it on a proper legal basis. Essentially, my check relates to all intrusive activities apart from interception. Some of those activities are the subject of the draft Bill—that is to say, the equipment interference—but others are not. For example, intrusive surveillance is not the subject of the Bill. I have oversight of two other areas: the first is bulk personal data, which is dealt with in detail in the Bill; and the second is consolidated guidance and the application of the Guidance, which, although it is not in the Bill, will presumably have to be taken over by the oversight body that is forecast by the Bill.

If I may say this in relation to the Bill, I think the present system works very well and provides safeguards. I say that because I see the agencies taking lawfulness very seriously and by taking authorisations very seriously, and I see the same among Ministers and in departments. But I can obviously see that it is impossible to explain exactly what I do very easily to the public, and that therefore there are members of the public who may not have confidence in the system that looks at things after the event, so I can see the merit of having judicial oversight. The way the Bill has it is right: that is to say, the Minister takes the decision and then there is judicial review of that decision. To that extent, I support that aspect of the Bill.

The Chairman: Thank you very much. That was most useful.

Q40 Lord Butler of Brockwell: Sir Mark, having had the privilege of often having you as a witness at the Intelligence and Security Committee, could I pursue the point you have just made? You have said, and certainly from my observation I would agree, that the present system has worked well. On the other hand, having three commissioners has not been widely understood by the public, and that is a fault. In the way it has actually worked, has there been, in your experience, any confusion between the three commissioners as to your separate roles? Indeed, has there been any overlap?

Sir Mark Waller: I do not think there has been any confusion between the commissioners, but there are areas of overlap, undoubtedly. For example, under the present scheme, you may go and get a property warrant, which is ultimately going to lead to an interception warrant. To that extent, in one sense, two commissioners are looking at the same exercise, so there is some overlap. But I do not think there is any confusion. We and the interception commissioner share an office, for example, so it is quite easy—if there is a problem, one can address it. I have never found confusion with Sir Christopher Rose, and now Lord Judge.

Lord Butler of Brockwell: Would you be satisfied with a system in which the new proposed Investigatory Powers Commissioner took over all the roles of the three commissioners? Does that need any further amendment to the Bill, or is the Bill satisfactory in that respect?

Sir Mark Waller: The trouble with one commissioner trying to deal with what all three commissioners deal with at the moment is that it is just far too much for one man. In relation to what I do, I am paid for something like 140 days in the year. The interception commissioner is paid for a certain number—I do not know what his days are—and then you have the surveillance commissioner. Frankly, although that is all I am doing, as it were, it is more than enough for me. I also worry, to be quite honest, about whether I would like to do the job I am doing 100% of my working time in a year. I am not sure I would. I do not know how to put it, really, but you have to probe and probe, and do your reading. Would I like to be going from one week into the next week all the time? No, I do not think I would. I would find difficulty in thinking that one person could cope.

Lord Butler of Brockwell: Did I understand you right when you said at the beginning that there is one form of intrusive surveillance that is not covered in the present Bill? If I did, should it be?

Sir Mark Waller: In my view, there is an inconsistency if you do not. It is fair to say that it will be covered by the same system that I say works very well, but there is an inconsistency. If you think in terms of intercept being an intrusion into privacy, surely the bug in somebody's house or somebody's flat is just as intrusive. It is difficult to think that it is not. I do not quite know David Anderson's view on this, but, given his previous view that you needed judicial authorisation, I would have thought it must be the same in that area.

Lord Butler of Brockwell: You are telling us that, at the moment, the placing of a bug in the entrance into somebody's premises is not covered by the system proposed by the Bill.

Sir Mark Waller: That is right, although I think one ought to emphasise that it can happen by virtue of equipment interference. Of course, if there is some equipment interference, that is covered by the Bill; but, if you are just looking at a bug under a sofa or whatever it might be, as I understand it, that is not covered by the Bill.

Lord Henley: Lord Chairman, I am very grateful for you allowing me to come in now. I was going to come in later on, but, after Lord Butler's questions, I just wanted to ask Sir Mark whether he could say more on what he thought about the extra costs of what is being proposed. Is it going to be that much more expensive; if so, why; and is that justified?

Sir Mark Waller: Let us take those one by one. Why is it going to be more expensive? Well, as I understand it, the costs are assessed on the basis that you are going to have this body, plus the top person and at least four judicial commissioners. I would have thought that was an underestimate. I do not know how they reach the present figures, but it seems to me that that is likely to be an underestimate. If you say that somebody is going to have to look at 100% of the warrants and authorisations, you have already multiplied the task that either the interception commissioner or I do. The interception commissioner talks about 50% in terms of the review; I look at something in the region of 17%. I see the total description of what a warrant involved, and I see 100% of those, but in terms of looking at the paperwork that lies behind it, as anybody who is conducting a judicial review of a decision of the Minister will have to do, in my time I only managed to look at some 17%. If you say, "No, you have to do 100%", that is a massive amount of extra time. You asked me whether I thought it was justified; I do not think it is.

The difficulty, which I understand, is that the public perception is not satisfied by an after-event review. I suggested at one time that you might do it by simply notifying a judicial commissioner of every warrant that is issued, giving the commissioner the opportunity to look at it, and him or her having a staff who would point up to them anything that looked problematical.

I am going to say something more that is not in answer to your question. There is a lot of concentration on the authorisation process. My judgment is that people should not be so concerned about the agencies wanting to act unlawfully; they do not. What has to be watched is that there may be a rogue in the agencies who might use the very powerful methods that are available. Rogues do not go and get warrants. One thing that certainly must not get lost in all of this is the oversight required to see that the agencies have the structure and methods in place to ensure there are not rogues, and that anybody doing something in the agency cannot do it without other people seeing. That, in my judgment, is more important than the authorisation process.

The Chairman: That is a very interesting point; I totally agree. You mentioned earlier on that you saw the difficulty of replacing three commissioners with one. Of course, the new structure is that of a single commissioner, but with a team of commissioners working for him or her. What about the problems, though, in the work you currently do as the Intelligence Services Commissioner? We have touched on what they are and how they are different from intercept. Do you think that any of that could get lost in the restructuring, in that there is not a specific Intelligence Services Commissioner in the sense of what you do, as opposed to your replacement? In other words, your replacement has an overall brief for everything, whereas you are specifically dealing with non-intercept surveillance of one sort or another. How do you think that would work out?

Sir Mark Waller: I hope the Investigatory Powers Commissioner would understand that it is important to have a senior judicial figure in charge of each particular area, including the

ones over which I have oversight at the moment. I would have thought that was key. If that happens, there is absolutely no reason why that which I oversee should get lost.

Q41 Lord Strasburger: Sir Mark, it might help us understand your concerns about workload a little better if you tell us how many staff you have working for you and their levels of technical expertise, in particular in relation to CNE.

Sir Mark Waller: I now have three staff, although for a lot of the time I have been operating with one. Technical expertise, no, but we go down and learn from GCHQ, for example, about the CNE activity. I am not too troubled about the fact that I do not have technical expertise, because, in terms of checking what I am checking, which is whether intrusion into privacy is justified, I do not see that I have to have that technical expertise. That does not worry me so much. I also think that the strength of the system I am responsible for at the moment is that I do it. I do not have individuals going in who are not judges; I read the documents, and I am analysing whether the case is made out or not. Maybe I am wrong, but I think that is one of the things that the agencies appreciate and why they take the authorisation process so seriously.

Lord Strasburger: Just for clarification, you are saying that neither you nor any of your staff have expertise in CNE.

Sir Mark Waller: Not technical expertise, no. That is absolutely fair.

Suella Fernandes: Just to follow up, what is your view on the proposal that the new regime of commissioners will be supported by technical experts, will have in-house legal teams and will have the option to buy out extra specialist advice like legal counsel?

Sir Mark Waller: If I am absolutely honest, I do not believe it is that necessary. I have been dealing with the CNE activity and with the intrusive aspects, and all I can say is that I do not feel I am in any difficulty in understanding exactly what they are seeking the authorisation to do. I can see it. The question is: "Have you made a case that it is necessary to do that?". I read that case and see it made.

Then the next question is: "Is there an intrusion into privacy?". The answer is that there will be in relation to the target, but you have to look at whether there is collateral intrusion, because whatever you are attacking may be used by other people. You then look to see, first, whether they have methods by which they keep that to an absolute minimum; and, secondly, whether they have procedures in place to destroy or not look at the material that has been obtained and that they do not need. I do not believe I need a great deal of technical expertise in order to make those judgments, but others take a different view.

Suella Fernandes: That was by way of follow-up. To put the actual question I wanted to ask, what is your opinion of the proposed new authorisation regime for warrants, including review, in comparison to the old? Do you think it provides a better form of safeguard?

Sir Mark Waller: If you have a judge looking at 100% of the warrants, one cannot but say that it must be better. Do I think the safeguards will actually be greater? I do not think they will, but I think the public require something that is pre-event. Although I think the present

system works, I can see that you may need something before the event, which the present system does not have.

Suella Fernandes: I am sensing from your response that it is more that justice is seen to be done by the public, and that is the sole reason the judicial element is included, but the qualitative, substantive nature of the decision-making is not necessarily going to be enhanced.

Sir Mark Waller: When you say "justice", it is a matter of the public having confidence. The agencies require very intrusive measures and this Bill is adding to them. I completely understand that the public have to have confidence and that that should involve judicial review at the pre-event stage.

Q42 **Baroness Browning:** Could I ask you about training for the new judicial commissioners? Presumably they will be required to be subject to a vetting procedure despite the fact they have held high office as judges, we understand.

Sir Mark Waller: I doubt it.

Baroness Browning: You doubt they will be vetted.

Sir Mark Waller: I was not, and none of the commissioners, as far as I know, ever have been.

Baroness Browning: Do you think that is a good idea?

Sir Mark Waller: To be honest, it has never worried me, since I was not vetted.

Baroness Browning: Can I worry you now?

Sir Mark Waller: No, I do not think you can worry me, honestly. Remember, we are talking about people many of whom will have sat in the Court of Appeal. They will have had before them cases involving secret material. They are not vetted for that purpose. They are strictly trained in terms of having safes, which they have to have in their room, and they have to go through all the procedures, et cetera. Maybe somebody has been secretly vetting—but, as far as I know, they are not vetted.

Baroness Browning: As to the training element, presumably these will not be people who have expertise in this field to the degree to which they are going to need to apply it. How do you envisage the sort of training needed and, from your own experience, what would be helpful by way of training?

Sir Mark Waller: I can only speak in relation to my position. I am not quite sure what sort of training you have in mind. My predecessor was Sir Peter Gibson. I shadowed him for a period of months before I took on the job, and I went down to the various agencies to discover exactly what it was they were being authorised to do and how it worked. I visited Ministers' offices as well. At the end of the day, I do not believe my task requires a great deal of training beyond that which I have already had as a judge, in that I am looking to see what case has been made for getting an authorisation.

That is set out sometimes at too great a length, but, on the whole, at length anyway. First of all, it sets out the case of necessity. It is easy for me to judge whether that is a case that has been properly made. Then the second area I am concerned about is proportionality, which is the intrusion of privacy. Once again, it is possible for me to see, first, how that has been limited; and, secondly, at the end of the day, when there is some intrusion into privacy, how that has been justified by the necessity case. I suppose I would have quite liked to go to school and have somebody teach me all that, but I do not think it required me to do so.

Q43 Lord Hart of Chilton: There has been some criticism of the judicial review principles by Andy Burnham and David Davis, who said that the judicial review test gives judges too little power because it only relates to process. David Pannick, on the other hand, has written an article saying, no, that is not right, because it allows a judge full power to look at the merits of a case. I assume by that he means that you could look at it from a Wednesbury point of view as to whether the Secretary of State had properly and reasonably come to the conclusion that he did. I wonder if you can help us a little further in looking at the factors that judicial review would take into account from a commissioner's point of view.

Sir Mark Waller: I thought Lord Pannick's article absolutely hit it on the head, in the sense that he said a judge should have vigilance, to make sure the agency is acting within its power and adopting the right test, and then circumspection, acknowledging the superior knowledge of the Executive in national security matters. What I do and what I would understand a judicial commissioner to have to do is, first of all, look to see whether a case of necessity is made. To put that another way, would a reasonable Minister take the view that a case for necessity was made?

It is almost invariable that the case for necessity is made: they say that there is a terrorist or whatever it is. The real question that I concentrate on is the proportionality, because it seems to me that, even on a non-judicial review basis, you can look very carefully to see, first, the extent of invasion of privacy; secondly, whether there is collateral invasion of privacy; thirdly, whether somebody has measures under which they reduce that to the minimum; and, fourthly, whether they have properly balanced the necessity for getting the material against the invasion of privacy. I think a judge will—and I do—look very carefully at that last one. That is what I understand Lord Pannick to be saying: it is not quite as simple as saying, "Would a reasonable Minister", et cetera; you look very carefully at that last aspect because that is what you are being asked to look at.

Lord Hart of Chilton: So you think it can safely be described as a double lock system.

Sir Mark Waller: I say that for two reasons. The first is that what must worry members of the public is that these agencies are doing things outside their powers. There is no question but that a judge can look at that and, if they are acting beyond their powers, the judge will stop it. Secondly, because of the area we have just been dealing with, it seems to me that collateral intrusion particularly is something a judge is well capable of assessing, looking at and seeing that it has been properly dealt with. So it is a double lock, yes.

Q44 Matt Warman: It seems to me that the move from retrospective analysis of a decision to looking at it in advance is a shift, and it indicates that you could prevent something from happening rather than complain about it after it had happened. I wonder if you could give us

a sense of how often you have looked at things retrospectively and thought that they should not have happened.

Sir Mark Waller: There is one example in the whole of my time where I was troubled as to whether it should have. That was an occasion on which I went back to a Minister and I said, "I am troubled about that", and the Minister cancelled that warrant and produced another one. That is the only time in five years. As I say, the agencies, in my experience, are extremely keen to get this right. People would be surprised at the amount of documentation that lies behind each of these warrants, arguing out the case for necessity and for proportionality. Of course, also in these submissions is the risk that they may be found out or whatever. That is all there too, but the really important ones for review are necessity and proportionality.

Matt Warman: In practice, while this double lock would not change the decisions in all bar that one case, it would provide much greater reassurance to the public because it is happening in advance.

Sir Mark Waller: Exactly that.

Matt Warman: So there is a real benefit to doing it, as well as being seen to have a benefit to doing it.

Sir Mark Waller: Because of the confidence it gives to the public, yes.

Bishop of Chester: It surely feels different to have approval before the event, rather than review after the event. Culturally, it feels different, but you are saying in practice that there is not much difference.

Sir Mark Waller: No. I am agreeing with you that there is a difference, and it must give the public more confidence if the review is before the event, rather than after the event. I agree with that.

Bishop of Chester: In Lord Pannick's article, which I do not have here, he spoke of a margin of discretion or appreciation being part of the judicial review process. Does that mean that the commissioner is likely to give the Minister the benefit of the doubt?

Sir Mark Waller: In terms of necessity, I have no doubt that that would be right. In terms of proportionality, if it has not properly been dealt with in respect of invasion of privacy, I do not think there would be any question of giving the Minister the benefit of the doubt.

Q45 **Stuart C McDonald:** Sir Mark, I have just a couple of supplementary questions to things you said earlier. First of all, are there times when technical expertise or support could be useful: for example if you are considering proportionality and whether other forms of monitoring might be less invasive? Even where services are using measures to reduce the level of interference in someone's privacy, would it not be useful to have technical expertise or support?

Sir Mark Waller: I do not really think so. When someone wants to use a particularly intrusive method, they will say, in the submission dealing with proportionality, that they have considered these less intrusive methods and, for one reason or another, they cannot

use them, so they have taken the decision that the only way—and this is often the expression—they can get at this particular bit of information, which is vital for the necessity case, is by this method.

Stuart C McDonald: Is it not useful to have technical expertise, then, to be able to challenge and assess whether that is an accurate assertion?

Sir Mark Waller: What sort of technical expertise? I am sure I am not allowed to ask you questions, so I refrain from doing that, but I am not quite clear. Are you trying to say that nobody can do this oversight job or judge necessity and proportionality without effectively being a technical expert, a computer expert, a CNE expert?

Stuart C McDonald: Or having technical support, rather than just one member of staff.

Sir Mark Waller: Maybe I would increase my staff, and if somebody supplied me with a technical expert I suppose I would say, "That is very nice", but I am not sure how often I would use them.

Stuart C McDonald: Earlier on, you also emphasised how important it would be to have methods to ensure there were no rogues in these agencies. How do we go about doing that? What would the commissioner's role be in trying to make sure these methods were in place?

Sir Mark Waller: There are two ways in which I try to do it, anyway. The first is that, if I visit an agency or a station, I often at the end say, "I do not believe a single word you have told me. I think there is a room behind, in which people are operating without authority and just for their own ego. How do you show me that that is untrue?". It takes them a little by surprise, initially, but the reality is that they do explain how it is impossible because people cannot do things on their own. They have recognised the problem there will be if there is a rogue, and they make sure that nobody can operate any of the equipment they are talking about without somebody else knowing and without it having to go to senior people. I try to ensure that that process is in place.

I also try to ensure that they have a vetting process, which they obviously have to have at the beginning, before they employ somebody. You have to have a very good vetting process to make sure that you do not have rogues coming in. The real key is to make sure that nobody can operate without other people knowing.

Stuart C McDonald: I have two final questions, to provide public reassurance more than anything else. Who picks the warrants that you review? Who chooses which ones you have a look at?

Sir Mark Waller: I personally pick them. It is not a completely random pick, because I get a complete list of all the warrants and they have a subject-matter description, so, if I look and think, "Well, I wonder", I will pick that one. Otherwise, I pick at random.

Stuart C McDonald: Finally, earlier on, you said you were very confident that there was no systematic abuse within any of the agencies of the capabilities they have. Others are not quite so confident about that. Is there anything we can do to insure against an agency systematically going beyond the powers it has through warrants, for example? Is that possible? How would

we ever know if an agency was systematically just not applying for warrants or ignoring the scope of warrants?

Sir Mark Waller: Taking the first, if they are going to do this, they are not going to apply for warrants; they are going to do it without warrants. You have to be right that, if there was a conspiracy or a wickedness from the top of the agency down to the bottom, they could do things unwarranted, because they have very powerful kit to use. Can anything be done to prevent there being a conspiracy overall? The answer to that has to be: you must appoint good people at the top; make sure there is a good appointment process for the people working at the agencies; and have a system under which people cannot do things individually.

Mr David Hanson: To follow up on that question from Mr McDonald, did you see it as any part of your current role to undertake post-evaluation of the warrants that you agreed or authorised? Take, for example, the one you had difficulty with, where you subsequently authorised a revised warrant. Do you see it as any part of your current role to revisit the exercise of that warrant, or is that solely for the independent reviewer in due course?

Sir Mark Waller: I do that. I do not systematically say, "This is what I am going to do. These are the warrants for which I am going to look at the authorisation process. These are the ones I am going to look at in terms of whether the conditions have been properly applied". Obviously, in the course of one's inspections, one is looking at warrants again, and one will look to see whether the conditions on which they got the warrant have been complied with.

Mr David Hanson: Have there ever been occasions, then, on which you have felt subsequently that the authorisation requested and the authorisation given by yourself were disproportionate, subsequent to your approval?

Sir Mark Waller: No, there have not.

Mr David Hanson: The Bill itself, under Clause 176, provides for the Secretary of State to fund the judicial commissioner—

Sir Mark Waller: May I correct that last answer? Nobody should say that the agencies are completely perfect and do not make some mistakes, but they report errors, on the whole. I do not want there to be any misunderstanding. For example, there are occasions on which, by human error, somebody has allowed an authorisation to run out. I am not talking about a ministerial authorisation; I am talking about an internal authorisation. That is an error and, if they find it out, they have to report it. I may talk about it on the day when I go to inspect, or I may want to go and talk about it immediately, if it is something serious.

Mr David Hanson: I simply ask that question because I recall, in my previous ministerial life, undertaking an exercise of requesting a warrant, only to find that it was not subsequently used. Then a request came to renew it, and it was not subsequently used. It was an interesting reflection on how much assessment you make subsequently of the use of any particular power. That was all, but you have answered that question.

I will move on to the issue of funding. As I was mentioning, Clause 176 of the Bill provides that "The Secretary of State must, after consultation with the Investigatory Powers Commissioner and subject to the approval of the Treasury as to numbers of staff, provide the judicial commissioners with (a) such staff, and (b) such accommodation, equipment and other facilities"—this is the key point—"as the Secretary of State considers necessary". Does that in any way limit your subsequent independence, as it is the Secretary of State who determines the staff, accommodation, equipment and facilities?

Sir Mark Waller: I would have thought it would absolutely not limit independence. Their independence is ingrained in judges and I do not believe that the fact somebody has the purse strings, as it were, for the resources has any effect on independence. If it did not happen, it might have an effect on your ability to do the job, but that is rather different. I do not believe that the fact the Secretary of State ultimately holds the purse strings would affect anybody's independence.

Mr David Hanson: The question is about "such staff", for example. In theory, under Clause 176 of the Bill, a Secretary of State could determine that you were to have funding for particular types of staff. For example, we talked earlier about technical expertise. It may be that the Secretary of State deems that you do not need technical expertise, but ultimately you or a successor in a particular instance deems that you do. It is a question of whether the clause is sufficiently flexible to allow you to make those judgments within a budget, or whether the Secretary of State in any future regime could say, "We should have two support staff and one technical staff, and that is the funding I am giving". If you deem that you need additional technical support staff, Clause 176 deems that the Secretary of State determines that. That may or may not be a problem. I am simply asking, from your experience, is that a problem?

Sir Mark Waller: No, but I am slightly hesitant about it. At a time of austerity, one has had to fight to get one's staff. We have had to fight to get ours. On the whole, the answer is no, but I do stress that it is not something that is getting at the independence. It is something that just makes it more difficult to do the job.

Q46 **Bishop of Chester:** When you double-lock a door, the two locking mechanisms have to be completely independent, otherwise it is not a double lock, by definition, in a sense. I am interested in the fact that the Investigatory Powers Commissioner is appointed by the Executive—by the Prime Minister—and makes subsequent appointments of the commissioners. I am not saying individuals would not be independent because of the nature of their backgrounds, but would it seem to separate the two locks, as it were, if it were not the Executive making the appointment but the Lord Chief Justice or someone more judicial?

Sir Mark Waller: I thought that I had heard they were going to use the judicial—

Lord Butler of Brockwell: Judicial Appointments Commission.

Sir Mark Waller: Yes.

Bishop of Chester: The draft Bill says that the Prime Minister makes the appointment.

Sir Mark Waller: Right. That is the present position as far as commissioners go. It is the Prime Minister.

Bishop of Chester: In Clause 167 of the draft Bill, it is quite clear it is the Prime Minister. Each commissioner, including the senior commissioner, is just appointed for three years, and if the Executive do not like how that person has been doing their job, without any further explanation they do not have to reappoint. Three years is quite a short period. I would be interested in your comments.

Sir Mark Waller: All I can say from my experience is that my being appointed by the Prime Minister has not made any difference to my role and what I do. I was not nervous, when I was coming to the end of my three years, about whether I might be reappointed or might not. It did not occur to me; I just did my job. If I may say so, there is a public perception point here, which you may be right about. I honestly had not thought that one through. There might be a public perception point. It might be better to have an independent body appointing.

The Chairman: Sir Mark, we are very grateful to you. It was a very interesting and useful discussion, and will help us considerably in our deliberations.

Sir Mark Waller: Thank you, Lord Chairman, for having me.

Simon Miller, 3 (QQ 145-161)

Evidence heard in public Questions 145-161

Oral Evidence

Taken before the Joint Committee

on Monday 14 December 2015

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, Mr David Hanson MP, Stuart C McDonald MP, Matt Warman MP, Baroness Browning , Lord Butler of Brockwell, Bishop of Chester, Lord Henley, and Lord Strasburger.

Witness: **Simon Miller**, 3, gave evidence.

Q145 The Chairman: A very warm welcome to all four of you. As I explained to our colleagues who came in earlier this afternoon, this is a hugely important Bill. We are very grateful to you all for coming along so that we can ask for your views about it and you can put any points to us that you wish. I am going to kick off by asking all of you how extensively the Home Office has engaged with you with respect to this Bill.

Mark Hughes: It is fair to say that Vodafone has had a number of meetings with the Home Office over an extended period. The engagement has definitely been better this time than it was in the previous Communications Data Bill period. It is also fair to say that we still have concerns over a number of aspects of the Bill, so we hope to be able to talk some of those through today.

The Chairman: Generally speaking, you are satisfied with the engagement.

Mark Hughes: Yes.

Simon Miller: Before I answer the question directly, it is probably worth emphasising how importantly we regard all our customers' data security, both in terms of keeping it safe from attack and in terms of how we process it to provide the service and experience our customers want and need, which is done strictly in accordance with law. The levels of engagement have broadly been good. They have certainly been far more extensive than anything we had experienced before from the Home Office and certainly much better than for DRIPA. The engagement has taken a number of forms—and I hope I am not speaking for everyone else here—including large roundtables with the Home Secretary, timetabled sessions and informal bilateral and multilateral meetings.

The one area that has been lacking is tripartite discussions between us as communications service providers and law enforcement agencies, together with the Home Office. It is also true to say that, although the level of engagement has been good, the iterative approach to consultation has revealed a significant number of issues with the legislative proposal that the Home Office has yet to address or has not addressed. These will be fleshed out, I am certain, in the course of this session.

The Chairman: I am sure you are right.

Jonathan Grayling: To echo that, engagement has been positive and significantly better than the Communications Data Bill. There have been some regular timetabled sessions. They have been cross-stakeholder, involving law enforcement, industry and the Home Office. That has been really useful, because it has assisted in providing a common understanding of operational requirements, technical capabilities and policy drafting. That said, this is a piece of government legislation and it is ultimately Parliament's decision what is and what is not included in the Bill. EE's main priority is our customers' privacy, and as such there are still a number of areas in the Bill that we have some concerns about, which we hope we can bring out in the next hour or so.

Adrian Gorham: I will not repeat the comments my colleagues have made, but it is certainly much better than we have seen in previous legislation that has gone through, so we are very pleased about that. We have had a good level of debate.

The Chairman: That is an interesting start.

Q146 Lord Henley: It is very pleasing to hear that the Home Office has been consulting, speaking as one of the various former Home Office Ministers on this Committee. We understand there is a shortage of IP addresses, and we also understand you do not always record which subscriber had which IP address and which port number at any specific time. What can you tell us about the practical difficulties and the costs that might be incurred in conducting IP resolution?

Adrian Gorham: When they developed the IPv4 standard, there were 4.3 million addresses worldwide, so that clearly was not enough, as technology took off, to give each customer an individual IP address. When the mobile phone business moved into doing internet connections, we had to come up with a solution to that, because we could not give every customer their own unique IP address. They developed a technology called network address translation, which means that every time you go on to the internet and have a data session, you are given an IP address, for a very short period, for that transaction, and then it just drops off. The next time you do something, you are allocated another one, so it is very dynamic and it changes all the time.

We had no reason to make a record of that. That is our challenge. We now need to record what number we allocate to each session and store it, and build the devices so that we can disclose that to the authorities.

Jonathan Grayling: To pick up on Mr Gorham's comments, the key point here is that at the moment the technology does not exist to be able to resolve that IP address. The public-facing IP address could have multiple thousands of unique devices attached to it. Indeed, trying to resolve that public-facing IP address to at least a near one-to-one match—and that is Parliament's intention—will require the retention of internet connection records.

As I said, the technology does not exist at the moment. We are in the feasibility stage now. At the end of that feasibility stage, it will probably take up to 18 months to deliver a solution because of the complexity involved.

Simon Miller: There is not much to add to that, other than to say that the technical challenges faced by my colleagues at both O2 and EE are replicated across the board.

Mark Hughes: I have just one thing to add. Vodafone is in exactly the same boat. We do not keep the IP data of all our customers. We are going to have to deploy new technology to be able to do this. The other thing that has not been said so far is that we will need a very big storage system to be able to keep it. It is a significant amount of storage.

Q147 Lord Butler of Brockwell: Could I take a step back and ask about the existing system and the requests you get for call data records under Sections 21 and 22 of RIPA? We know that is a diminishing resource as far as the intelligence agencies and law agencies are concerned, but are you satisfied that, to the extent you still have those records, that system works reasonably well?

Jonathan Grayling: Yes, the current acquisition arrangements under RIPA work well. One of the primary provisions, which is tried and tested, is the SPOC system. Essentially, that is the provision of comms data to law enforcement and the SIAs to a single point of contact. The use of SPOCs provides a strong, transparent and stringent process. As I said, it has been tried and tested over many years. Their SPOCs are specially trained. They are accredited in the use of CD, so they can advise their respective officers within law enforcement and the SIAs on what CD needs to be acquired.

That said, we also welcome the additional safeguards in the Bill. We welcome the requirement for a designated person, independent from the requesting agency; the streamlining of existing legislation and repeal of old legislation, so the Investigatory Powers Bill will be the primary piece of legislation for the disclosure of CD; and the restriction of ICRs to certain authorities and for certain purposes. Moving into the IP world, keeping the SPOC community and law enforcement up to speed with new technology is going to be a challenge, and a significant amount of effort will be involved in ensuring that law enforcement and SPOCs can interpret the data that we are talking about today.

Lord Butler of Brockwell: Going forward, then, into the new world—you have begun to describe the complexity to us—is it practicable, by using the internet connection records, to distinguish just the first line of the address, which is what the Government want to do, and to draw a line between that and what would be more revealing about the content?

Mark Hughes: This is where we get into some of the more technically challenging areas of the Bill, for sure. It is important that we call this out as it is. We are talking here about web browsing data when we talk about internet connection records, so we need to recognise that this is a hugely sensitive part of the capability that is looking to be developed. In terms of how easy it is, this is where we start needing to talk about over-the-top or third-party service providers, who may be running their communication services under the underlying network providers that are here today.

To try to bring this alive with an example, Vodafone and everyone else here will act very much like a postman today. We would carry a packet of data, or a letter in this scenario,

from point A to point B at an IP address. We do not know what is contained in the letter in this scenario. In future, the challenge for us is having to open that letter. Let us say it is a Skype service. We would have to say, "Okay, now we have opened it, we understand that a Skype service is being provided", and the Skype username or ID of the person would be within that. You can already start to see how the lines are being blurred between traffic data and content when you start having to open packets of data as they cross the internet.

One of the main concerns here, especially around third-party data, is that, today, Vodafone has no day-to-day business use for this data. We do not create it, so we are going to have to generate new data about our customers that we do not generate today. Secondly, we do not understand its structure. That structure can change on a day-to-day basis, and it is encrypted, so we will have to be able to strip off the electronic protection and decrypt it before we can store it. We would be concerned about attesting to the accuracy of that information as well. I am also concerned about possibly creating a single point of cyber vulnerability when you start decrypting things to be able to store them. There is a very good reason why they are encrypted in the first place. I am concerned that we will perhaps solve one problem, but not necessarily in the best way, and create another cybersecurity problem. Our point is that the very best people to keep data about the services being provided are the third parties. They should be the people who are keeping information to help law enforcement fight crime in this country, rather than the underlying service providers.

Lord Butler of Brockwell: Give me an example of what you mean by the third parties.

Mark Hughes: I gave you an example there. It could be a Skype; it could be WhatsApp. It is those types of service providers.

Lord Butler of Brockwell: I see, so the people for whom you are carrying the traffic. Okay. You have talked about this being a very complicated process. Can you give us some idea of the costs?

Mark Hughes: Until we have been served with a notice, I would be purely speculating as to the cost. I would be uncomfortable giving you any kind of idea until the Home Office has served us with a notice. It would be significant, it is fair to say.

Lord Butler of Brockwell: The Home Office produced a figure, if I remember correctly, of about £180 million. Do you think that is an overestimate or an underestimate?

Mark Hughes: Where this figure from the Home Office came from I cannot say, because we were not consulted when it was put together. We were consulted only after that figure was put together. I would not be able to speculate, from a Vodafone perspective, as to how much it would cost.

The Chairman: Would all four of you agree that the cost implications are considerable, significant, huge, something you can manage, or you do not know at this stage?

Adrian Gorham: It is going to be huge. Also, there is the way data is exploding. The increase in data is about 100% per year. That is the big issue with costs; this is going to double by

next year, with the way the internet is going. There are going to be big increases in the future, with huge amounts of data.

Jonathan Grayling: I agree. Going back to what Mr Hughes and Vodafone said, unless we can be explicit in the Bill about exactly what data we are going to be required to retain in any future data retention notices, it is simply not possible to give a figure. If there is, within the legislation, scope that third-party data falls into our areas of responsibility, the costs will be even more. We are only focusing on the data that we understand now, the data that traverses our network, the data that we require in order to route a communication and provide a service to our customers. Even then, it is incredibly difficult to come up with a cost.

Q148 Lord Butler of Brockwell: I have one final question. I get the impression that you are not enthusiastic about this provision in the legislation. You think it is a lot of work. Even if the Government meet the costs for you, you are not enthusiastic participants.

Mark Hughes: It is not necessarily about being enthusiastic. We absolutely recognise the challenge that law enforcement and Government have here. Vodafone's concerns are very much about making sure that we have a Bill that is technically workable. At the moment we are really concerned about being able to keep data about a service that is nothing to do with our core business, generating new data about our customers and especially stripping off electronic protection and decrypting communications passing through the internet. This is a highly challenging arena for any of the companies here today in which to do things on behalf of somebody else's communications services. We feel that the third parties providing those services have an obligation here to assist law enforcement fight crime.

Q149 Bishop of Chester: Clause 193 gives a series of definitions in the Bill. One of the issues we have been wrestling with is the distinction between data and content. That is in subsection (6). Are you comfortable with that distinction between data and content in the context you are describing?

Jonathan Grayling: This is an incredibly complex area and, with respect to the Home Office, it is even more complex to try to define within a piece of legislation. Without wishing to go over the ground we have just covered, there are issues in relation to what is perceived as content and what is perceived as CD with respect to who owns that data. The definitions provide a basis for further discussion. It is a starting point, and it is a starting point for defining those capabilities. That said, echoing what we have just spoken about, to a CSP, to a network provider, the communications data is the data that is available to us that we see in order to provide a service to our customers. Essentially, that is the data we need in order to route a communication that we will process and that we will make a decision on. If we do not make a decision on that data, we do not perceive that as being our data. It is simply data attached to a packet, but the data within a packet could be communications data to the sender of that packet.

Again, if you talk about WhatsApp, all we are interested in doing is sending the WhatsApp message that traverses our network to the WhatsApp server. If you were to open that WhatsApp message, you might find out to whom that message was being sent, but we have no need to know that; we are just sending it to the WhatsApp server. That data could, to WhatsApp, be perceived as communications data, but, because we have to open the

packet, it is content to us. This is where there are blurred lines and why we are looking for clarity in the Bill as to exactly what data we should be required to retain as communications service providers.

Adrian Gorham: To build on Mr Grayling's point, another issue here will be the encryption, because so much of the data now going over our networks is encrypted by those application providers. In a lot of cases, we cannot see what is contained within that traffic. They are not going to give us the keys so that we can decrypt it to examine it, so in a lot of cases we are completely blind to that traffic.

Simon Miller: The issue here is that there is a clear need for further discussion with the Home Office to arrive at a text that works. There may be a need for further interpretive text, potentially in the Bill, but there is definitely a need for more than there is currently. The introduction of the ideas in the Bill is useful, but they need further unpacking.

Bishop of Chester: Do you think your customers would make that distinction between content and data, or would they think that the data is quite personal to them, quite apart from the content?

Mark Hughes: We know that customers would expect all the companies here today to look after personal information to the highest levels possible. Concerns about decrypting third-party communications as they cross the network would be of a concern. Again, it touches on the point that the persons who should have the obligation here are the third parties. They do not need to break the encryption because they have created the communication in the first place.

Q150 Lord Strasburger: Putting the last two topics together, encryption and degree of difficulty, with the proportion of internet traffic that is encrypted increasing by the day, is it possible that you will end up in 18 months' time with an expensive and rather complex system to collect these internet connection records, a diminishing part of which is of any use because encryption has increased?

Jonathan Grayling: That is a real risk. Technology is moving on so quickly. New protocols, new algorithms on the internet, are being created all the time, which makes it very difficult for us to see those communications. Yes, you have encryption, but you just have the way the internet is developing in itself. I would not like to talk about timescales and I would not like to comment on the actual benefits that the technical provisions we are introducing would give to operational law enforcement and the SIAs, but it is a risk that technology is moving so quickly that we may be behind the curve.

Q151 Baroness Browning: The three-level categorisation of communication in the RIPA legislation has been replaced by two: entity data and events data. Do you feel that reducing these categories down to two levels causes a problem? Are they sufficiently clear and workable? Is that a good thing? Is that going to cause you problems?

Adrian Gorham: In its simplest form, it does not cause us a problem. There are going to be two types of data. There will be entity data, which is about the actual person; it will be your name, your address, your telephone number, so it is about the individual. Then there will be the events data, which describes the event and will be about where something took place, the location. The good thing about those two fields is that a different level of

authority is needed by the police if they want that data. If it is about you as an individual, that will be authorised by an inspector, and if it is the broader data that includes the location, that will be signed off by a superintendent. That gives us clarity about what is required. The challenge is that as we move forward and more and more communications are coming online and more and more machine-to-machine, there will be different fields of data and we will have to have regular discussions to find out where those fields sit.

Mark Hughes: We were clear about the previous definitions. We are not clear why it needed to change, but we have no particular objections to the proposed changes.

Baroness Browning: With the advance in technology, are you referring to the fact that things that are not in use now but are coming up over the hill are things you will have to take decisions on?

Adrian Gorham: In the future, you are going to have SIMs in your fridge and your dishwasher. All these appliances are going to have SIMs in them that provide data. That all has to go into this process, and we are going to have to make those decisions where things sit.

Q152 Mr David Hanson: It is important in this session to try to nail down in some detail what you believe the Government are trying to do and whether you can deliver it. Could you just indicate to the Committee your understanding of internet connection records, as of the Bill's description?

Mark Hughes: It goes back to what I was talking about earlier. Internet connection records are web-browsing data, so they are not the page you end up landing on but the domain that you have visited. They do not exist today, so this is about us having to create and generate entirely new data sets.

Mr David Hanson: For Vodafone, how easy is it to deliver that new data set as of today?

Mark Hughes: It is extremely difficult, because, as we have heard, the vast majority of over-the-top service provider data that would be an internet connection record is encrypted and it is not data that we understand or in a structure that we have any understanding of, because we have not created it. We are now going to have to create an entirely new type of data on behalf of another company, decrypt it and then store it ready to disclose potentially in a court of law, where we cannot even attest to the accuracy of that information. It is very difficult.

Mr David Hanson: Vodafone is an international company. What demands are being made on you by other nations outside the UK in this field at the moment?

Mark Hughes: There is no standard approach internationally. There is a real patchwork, depending on the country. There is no one model. The UK model is certainly the most transparent, but there is no one model that fits all.

Mr David Hanson: What is other colleagues' understanding of what an internet connection is?

Adrian Gorham: This still has to be clearly defined.

Mr David Hanson: The Bill is in front of us now. Is it clearly defined for you in the Bill?

Adrian Gorham: We are nearly there on the clarification of what makes up the record. The challenge is that this is something we have never kept previously. We keep your CDR for every phone call you make. We keep the record, we store it for a year, and we can disclose it. This is a completely new kind of record that we are going to be keeping, and then we have to hold it, store it and disclose it, so it is a big step up for us in what we need to do and provide.

Simon Miller: The issue here is that we know that an internet connection record is going to be something like a simplified version of a browser history, but we do not know exactly what it is going to be. Until that bit is nailed down, we cannot ascribe a cost to it or know exactly how difficult it will be to implement. We do know that it is going to stretch our existing capability many times.

Jonathan Grayling: The key point here is that an internet connection record does not currently exist and we have to create it. Even once created, it may not exist as one whole record. As Mr Gorham said, we are beginning to get some clarity on what the Home Office believes an internet connection record may be made up of, the subsets of that internet connection record. Some of that data may or may not be retained. The issue is putting it all together to try to create something that is going to be of use.

Mr David Hanson: We are the draft Bill Committee. The real Bill Committee will meet in the Commons and the Lords, probably from the end of February until the end of July, and then this will be law. The question to all of you is: are you satisfied that, by the procedure of considering this in both Houses of Parliament, the definition, the deliverability and the apportionment of cost will have received sufficient attention to have confidence among your companies and the public that it is being done to the standard the Government expect?

Mark Hughes: Until the Home Office serves us with a notice as to exactly what it wants, it is difficult to speculate. We all understand it to be web browsing; we know that it is going to be difficult and challenging and that it will create lots of new data, which is going to be highly intrusive, but until we have a notice and know exactly what we have to keep about which companies, it is difficult to speculate.

Simon Miller: There has been a process of engagement in place that has got us this far and has led to improvements in what is being proposed. That suggests that it is possible to get this over the line. However, there are still a substantive number of challenges that need to be met in order to do that. At the moment, we have not necessarily had the responses from the Home Office that we either want or need on this in order to have full faith in that process.

Mr David Hanson: Is that the general view?

Jonathan Grayling: You cannot underestimate the complexity.

Mr David Hanson: Well, let us just go back to the point that Lord Butler made earlier about the costs, again, which the Government have estimated at approximately £170 million to £180 million. We had a panel in front of us last week in another Committee room who

basically said that they estimated that they had spent £170 million, just among the two to three companies in front of us that day. Again, it is important that you, either now or before the Bill reaches deliberation stage, as well as negotiating with the Home Office, are clear about the implications in relation to the costs. The Houses of Parliament cannot pass legislation that will not be deliverable, and it is going to have burdensome costs, on the taxpayer, the public, or both. Can you give the Committee any estimate now? Could you tell the Committee, "We think it is in the ballpark figure of X"?

Mark Hughes: Again, without wishing to be evasive on this question, it depends on how much of the internet traffic the Home Office wants us to keep. Is it every single third-party service? How quickly do they want it decrypted? How much of it needs to be stored? Is it for the full 12 months, like everything else? How much resilience does it need? Do we need one set of resilience, or do we need to be able to build it three times just to make sure that it goes down? Is it that important? It is those sorts of factors that can make this change from one number to something completely different at the other end. The only thing I can say, given what we know is in the Bill and what we know about the technology in this area, is that it will be a significant cost. Saying how much it will be would be me picking an item out of the air and literally speculating. It is going to be significant.

Mr David Hanson: I take it, by the looks of agreement and nods, that that is pretty much where the panellists are. Could I just then throw the other question in, which is still an important question? Ultimately, whatever the cost is fixed at—and you have said there will be a cost—who, in your view, is responsible for the apportionment of that cost? Is it something you take as a commercial issue? Is it something the Government have to fund 100%? Where do you land on that figure?

Jonathan Grayling: We believe that the Bill should make it explicit that a company impacted by this legislation is fully able to recover the costs incurred. We believe that if there is no cap on costs based on a proportionality aspect, and the obligation and the financial impact is simply passed on to the CSP, this could result in delivering disproportionate solutions. If there is a cost recovery model that places a cap on cost and is based upon proportionality, that provides a far safer investment for taxpayers' money and the privacy of our customers.

Q153 **Mr David Hanson:** Is there any disagreement with that? No. I have one final set of questions. Ultimately, if it is doable, if it is defined, if it is delivered, and if it costs something, at some point a police officer or agency is going to ask you for information. Are you satisfied that the Bill has sufficient provision in relation to the single point of contact from officers? Is that sufficient to give your customers and you the security you believe you would need?

Jonathan Grayling: It goes back to the point that until we know exactly what data we are required to retain and the format that it is going to be stored in, it is impossible for us to say whether a SPOC or a police officer is going to be able to interpret that data, because that data does not exist at the moment. That record simply does not exist, so we cannot say whether a SPOC community is going to be able to interpret, because we do not know what they are going to be able to interpret yet.

Mark Hughes: It is fair to say that the SPOC community will have to undergo an extensive amount of retraining to be able to understand this and make use of it in a day-to-day

investigation, especially considering how quickly, sometimes, they have to be able to make a decision based on this data in grave situations.

Mr David Hanson: I will come back to the final point: this could be law, in one form or another, by September 2016. What is your assessment of the deliverability, as of today, of the Bill as it stands?

Adrian Gorham: We would all accept that this is a big step up in capability. Everybody understands the challenge that the police and the security agencies have, and we all understand the capability gap they have with modern communications. This is going to be a step change for us, and that is why the discussions we are having with the Home Office are quite detailed, because we need to get this right. I am sure that everybody else on this panel, as well as me, wants to make this work and to ensure that taxpayers get good value for money. The only way we can do that is by having the strong discussions now, so we are very clear on what we need to provide and we do that in the most cost-effective way.

Mark Hughes: Regarding deliverability, without wishing to keep harping on about the same point, the easiest and most elegant way to deliver this capability is for over-the-top service providers to have the same obligations as companies here do today to assist law enforcement with information about customers who are using their services who may be breaking the law.

Q154 Lord Strasburger: On the subject of deliverability, Mr Hughes, you have twice said, "Then we will have to decrypt the data". How can you possibly do that unless you get co-operation from over-the-top providers, such as Facebook and others, or you get sufficient information from them as to how to decrypt that data, or from end users regarding how to decrypt their data? How can you do this?

Mark Hughes: You are absolutely right. The point of this is that we will have to be supplied with new technology, from law enforcement or intelligence agencies, to be able to decrypt that information about third parties and store it. That goes back to the point, again, that it is not preferable for our companies—certainly not for Vodafone—to be able to decrypt communications and store this. It would be much more elegant for the third-party service providers to have this obligation to assist law enforcement to fight crime.

Lord Strasburger: Presumably, by treaty, bearing in mind that most of them are American.

Mark Hughes: The Bill itself allows the Home Secretary to place an obligation on any person. Most, if not all, providers—certainly the big ones—have infrastructure and offices here. Given the way the internet is structured, there are things globally; I see no reason why the third parties would not want to assist with helping law enforcement in this space.

Stuart C McDonald: Mr Hughes, I think you said that you would not be able to attest to the accuracy of ICRs. Is that because of this process of decryption, or are there other reasons why you would not be able to do so?

Mark Hughes: It is fair to say that if we were able to extract data belonging to another provider, not understanding its structure as it crosses our network, I would be

uncomfortable with being able to explain the accuracy of another company's data. That would be an incredibly difficult thing for Vodafone to do.

Stuart C McDonald: So you might not be able to come up with accurate ICRs at all.

Mark Hughes: An ICR does not exist today. Once it is created and we have solved all the technical challenges that we have already discussed, I would imagine that it would be tested in court once this evidence becomes as bread-and-butter to the criminal justice system as mobile phone evidence is. I would imagine that it will be tested very heavily on the grounds of, "Who created it? How did you decrypt it? How accurate is it? If you did not create it, how can you attest to the accuracy of it?" Companies here, such as Vodafone, have to attend court to be cross-examined on mobile phone evidence that has been collected. We would find it extremely awkward to have to attest to the accuracy of data that we had not created in the first place.

Suella Fernandes: You appreciate, do you not, that the current lack in capability—for example, the requirement to keep internet connection records, or store them—means that the agencies can paint only a fragmented picture of a known suspect?

Mark Hughes: I absolutely recognise that.

Q155 **Suella Fernandes**: Examples abound, but in a recent referral of 6,000 profiles from the Child Exploitation and Online Protection command to the NCA, around 800 of those could not be progressed because of the lack of this capability. That is about 800 suspected paedophiles who were involved in the distribution of indecent images whose details cannot be gathered by the agencies. Bearing in mind the benefit that is gained by this storage and retention requirement, what alternatives do you think are viable while providing a similar benefit?

Jonathan Grayling: We are not necessarily questioning that there is an operational case for this. We work closely with the NCA; we work closely with CEOP. We are just trying to reflect the technical complexity involved in meeting the demands of law enforcement. We all have a duty of care as operators; we want to be good corporate citizens as well, but if the technical complexities are there, those are the facts, and we are trying to work through those with the Home Office to provide the provision that they are looking for.

The point that you raise there about CEOP goes back to the point about the knowledge of the law enforcement community. Certainly, the NCA are pretty advanced through the CEOP side of things in relation to trying to highlight these gaps in technology, and we work very closely with them on trying to close those gaps, but it is proving very, very difficult. The technology just does not exist at the moment.

Mark Hughes: I absolutely recognise what you are saying. We care passionately about assisting law enforcement. We take extremely seriously all the obligations that are placed upon us, and we do everything we can to give the best service to law enforcement through the system, with the things that we are obligated to do by law. As Mr Grayling has just said, we want to make sure that when this legislation passes and it has gone through the correct level of scrutiny, the obligations are technically workable and we can continue to provide the level of service that the police and law enforcement agencies expect from us. We get

how important this stuff is, and we really want to make sure that we can provide the data in the best way. Again, so much of this is going to be about over-the-top service providers that we must make sure it is achieved in the simplest way possible, and the simplest way possible is for those third parties to co-operate with law enforcement.

Suella Fernandes: In terms of maintaining the security of stored data, you use firewalls and personal vetting systems, and those are effective ways of keeping data secure.

Adrian Gorham: All the operators here are very experienced at looking after our customer data. We all have a layered approach; there are different systems and processes for keeping it secure. All this means is that we are going to have even more data that we will have to keep secure.

Interestingly, one of the parts of the Bill talks about a request filter, which will be run by a third party; a third party will take bulk data from us and analyse it for the police, to make sure the police only see the data they require. My concern there would be that that third party has exactly the same level of security that we deploy ourselves in our businesses. A number of us have international standards; I would expect that third party to have that level of security, if it has my customer data. I would expect the governance that we are putting in place to go and do audits on that third party, and I would—if I am giving them my customer data—expect to be able to go and audit them myself, to ensure that they are living up to our standards as well.

We are all very used to looking after security and protecting that data, but we now, with this Bill, have a third party whom we would need to give data to, and we need to be very sure that the same level of security is deployed there as well.

Q156 **Suella Fernandes**: Lastly, retention is subject to stringent controls; it needs to be necessary, proportionate, signed off by an independent person, and it needs to be compliant with various case law and the European Convention on Human Rights. What is your assessment of that consideration of lawfulness and effectiveness, combined with the exception of whether it is reasonably practical, as a sufficient safeguard to strike the right balance?

Adrian Gorham: The safeguards in the new legislation are very good. They are much improved on where we are now, and they are much more transparent. We have to ensure that the different auditing authorities do their roles and they are done properly. If you look at the recent audits they have just started doing on the operators with the ICO, they have agreed with industry what those audits will look like and what the definition and scope is going to be. The first actual audit was done last week on O2, so hopefully we will see the results of that come back. The one thing the Bill does very well is that it polices all the transparency in audit of what everybody is doing along that whole value chain.

Q157 **Victoria Atkins**: Mr Hughes, you have used the phrase "over-the-top providers" a lot. I may be the only person wondering this, but I suspect I am not: what do you mean by that?

Mark Hughes: The over-the-top providers I have referred to are companies that are running a communication service, such as WhatsApp, Snapchat, and Skype. They are examples of over-the-top service providers; they run a communications service using the underlying network providers that are here today.

Victoria Atkins: This is what I want to focus on. You have talked about how it would be more "elegant"—I think that was the word you used—for over-the-top providers to store this information, rather than you guys; sorry for being so informal. How on earth is law enforcement to know that one of the suspects that Ms Fernandes has referred to is on WhatsApp, Facebook or whatever unless they have that link in the middle, which is where you come in, signposting them to that application?

Mark Hughes: That is an excellent point. On signposting, we would have a role to play in saying, "We need to point you towards the company where you need to go to get the rest of the information about that customer", in a way they produce it and understand it. You make a good point about having to signpost the police in the first instance to what company has produced the communications service in question.

Victoria Atkins: If we just put that into the context of your evidence, you are not saying that your companies should play no role in this; you are worried about the details of decrypting and so on, but you understand that the Bill is phrased as it is to help law enforcement link a suspect to apps or services that they cannot know about unless you are involved in the middle.

Mark Hughes: Absolutely. This is about making sure that we do not blur the lines between traffic data and content by us having to open up all the packets of the data and then provide in an evidential way all the information to law enforcement.

Mr David Hanson: It is also about shifting the cost, is it not, from your perspective?

Mark Hughes: The Home Office has always had a policy of 100% cost recovery. They have assured us that this will continue. This is not an area that we make any money out of. We provide the very best service that we can to assist law enforcement.

Adrian Gorham: Another point worth making is that the customer of this is the police officer who wants the intelligence to allow him to make that arrest. If he believes that his target is using Facebook, the target may be using Facebook but it can use it on many different bearers. So it may use the O2 network; it can then go into a Costa Coffee and use a wi-fi network; it may then go somewhere else and use BT's wi-fi. It can use many different bearers, and you have to somehow get all that data from those different companies and put that all back together to show what that individual was doing on Facebook. If you go to Facebook and they have the encryption keys, they can tell you what is going on. They have all that data for that individual, so I do believe that it gives a much better service to the police to go to that one point of contact than try to go to each of the bearers that are carrying those communications.

Q158 Stuart C McDonald: You referred earlier to the process of setting up filter arrangements to get that communications data. What is your understanding about how request filters will work under this legislation, and would you have any concerns about the operation of request filters?

Simon Miller: We understand that the request filter is a mechanism by which large amounts of bulk or collateral data provided by us as communications service providers, as a consequence of requests made by law enforcement agencies, will be gradually—through a process of correlation and different data points—narrowed down to identify either a single

subscriber or a smaller subset of users, and that this will be done by a trusted third party. The whole purpose of this request filter is to minimise the amount of unnecessary bulk data that will be handed over to law enforcement agencies.

We are all agreed as to the principle of this. There are a number of concerns, which Mr Gorham has alluded to, regarding the detail. The first is the fact that we would still continue to provide bulk data to a third party, and in so doing could be in breach of our duty of care under the Data Protection Act and the Privacy and Electronic Communications Regulations to our customers' data. The second is that we have absolutely no detail on what this trusted third party would look like, the form it would take, or the legal obligations that it would be under. As a minimum, we would simply expect that whatever operation the request filter undertook was done to the same standards, and was as secure, as our own arrangements.

Stuart C McDonald: So you have no idea who these third parties would be at all.

Simon Miller: Not yet, no.

Stuart C McDonald: What exactly is the filter? Who is responsible for putting that together, and would you have any ability to review what the filter was doing to your data?

Mark Hughes: I do not know who would be providing the service. I think it would be for the Home Office to select a vendor, to be able to build that situation. In principle, it is a good idea to be able to prevent lots of collateral intrusion. When you have really big, complex inquiries that you are running as a police officer, where you may need lots of data, the filter can be a way of reducing the collateral intrusion. The important thing here, as Mr Miller just said, is that whoever operates that has to operate it to the same standard in terms of the data that is being provided out of it, because this could fundamentally change the way network operators give evidence in court. Remember: we are potentially providing information into the filter. The operation, and what changes in the middle and what ends up on a police officer's desk from the query they have run is being provided by a person in the middle, a third party service—a vendor in this scenario. Again, we would need to make sure. It is going to take a lot of close collaboration to make sure this works well.

Stuart C McDonald: What sort of things would you want to see in the Bill so that you could have faith in that filtering process by the time you arrive in court to speak for the accuracy of the data you have provided?

Mark Hughes: We want direction and understanding on which parts of the evidential chain we would be expected to stand up in court and be cross-examined on, and whether, if the data had changed in the middle in some way, it would be the third party—for example, in this case, the vendor who is providing the service—that needed to attend court. I appreciate that these are sort of in the weeds, and they are quite technical things that we need to be thinking about, but essentially we are giving evidence in court on a day-to-day basis on mobile phone evidence, and we are worried about making sure that we can continue to do that with what is essentially a new piece of kit in the middle of the network.

Simon Miller: At the moment, this may be an issue for guidance, but these are discussions that the Home Office is yet to have with us, so we are dealing with an unknown. We are very keen that these discussions continue, and that these issues are bottomed out.

Stuart C McDonald: Any further thoughts?

Jonathan Grayling: Just to reiterate, the panel has said that the Bill places an obligation to provide security controls in relation to retained data, and those security controls are audited and will be audited. What is not in the Bill is that there are similar security controls for the request filter, and subsequently the customer data—my customer data that I am supplying to the filter. I would like to see the filter having the same security controls as the ones CSPs are compelled to provide in relation to retained data.

Q159 **Matt Warman**: Can you say a bit about what you understand by a technical capability notice, and what you understand by the Home Secretary being able to impose one at will?

Mark Hughes: Our understanding is that this is about the potential for equipment interference. Vodafone has three real concerns about this particular item. First, equipment interference could obligate a network operator to introduce, say, a backdoor or a way to launch some kind of attack against a particular target that may be using the network. You will probably not be surprised to hear that we have three concerns. First, we are worried about this representing a real diminution in trust in UK-based service providers, which may have to introduce backdoors on their network. In such a highly competitive marketplace, if you had to decide who to place your communication service providers with—a UK-based company that potentially has this obligation, or somebody else who does not—you may be really thinking about that.

Secondly, we are concerned about an obligation that may ask us to fundamentally reduce the level of security of our products or services, or our networks. We would be really concerned about introducing any reduction in the level of security of our products and services. Thirdly, we understand that, as it is written in the Bill, this may involve our people and our staff having to get involved in launching such attacks against targets across our network. We would be keen to make sure that that does not happen, and it is down to the law enforcement or the agencies to manage the workable provisions of that.

Matt Warman: Any other thoughts?

Jonathan Grayling: I would echo what Vodafone said there. With respect to the Bill itself, there are a number of aspects of control and oversight over those technical capability notices that we do welcome—significantly, the fact that the Home Secretary has an obligation to consult with the respective CSP prior to serving a technical capability notice on that CSP. That consultation has to take into account, among other things, proportionality, technical feasibility, the cost—which is significant for us—and the impact on our customers and our network.

Even after that consultation process, and a notice is served, there is still a mechanism whereby if the CSP is still unhappy or concerned with that notice, they can pass it back to the Home Secretary for further review and, again, the Home Secretary has an obligation then to consult with the Technical Advisory Board and the IPC, which we welcome. The key point here is that we need to ensure that each stage of that process is rigorously enforced, rather than a rubber-stamping process. If we have concerns about that, we want to have it demonstrated that the appropriate oversight and controls are being applied to that process.

Just one very quick, final point. My understanding of the Bill is that the IPC would have responsibility for the oversight of national security notices. I cannot find anything in the Bill that says that the IPC would have oversight for technical capability notices, so the question is why that might be the case.

Matt Warman: What do you think your customers would make of even an oversight arrangement that you were corporately happy with?

Jonathan Grayling: Customer trust is essential to our business, and the priority for us is to ensure that we provide a secure and resilient network. That is what our customers will expect. If there are any powers or any activity that is undertaken by the agencies in relation to equipment interference, whether that is proportionate and lawful is a matter for Parliament and the agency itself, but EE would not accept it if those activities had any impact on the security of our customers' data or the resiliency of our networks.

Q160 **Matt Warman**: Moving on to the IPC that you mentioned, do you think that the level of engagement that is outlined in the Bill between you and the IPC is sufficient to maintain that level of security and trust?

Simon Miller: The levels of engagement envisaged are broadly similar to those that we have currently with existing authorities. Interject, gentlemen, if I am talking out of turn, but those levels are appropriate to the subjects concerned. The issue for us has always been that they are broadly uncoordinated, and as a consequence of that there are business impacts. In particular, at the margins, there are jurisdictional overlaps with different authorities talking to the same subject with different voices. It therefore follows that we are fully in favour of the creation of a single body, the IPC, that will have all these powers of oversight, and it will rest in that one body. The simple fact of the matter is that the current practice of having separate bodies with these different functions is, for us, broadly cumbersome, open to misinterpretation and misunderstanding, and time-consuming.

As for the actual level of engagement, this would be a new body. We would fully expect levels of engagement to ramp up as that body beds in and to have to adapt to new personnel and new ways of working. It is probably worth saying at this point that the relationship that we all have with IOCCO is an exemplar. If the IPC were to look at the ways of working exhibited by the existing authorities, it should look to IOCCO as a model of best practice, and we would very much like to see those practices demonstrated around building strong, coherent stakeholder relations, early engagement and demonstrating sector expertise continue.

Matt Warman: Broadly, it sounds as though you are looking forward to the changes that are coming, rather than dreading them.

Simon Miller: Absolutely.

Adrian Gorham: It might also be useful if there is an express right for the operators whereby if we have an issue or a complaint about one of the LEAs or the police we can go directly to the IPC to report that. That is not to say that there have been any issues previously with them, but it is worth having in the legislation so that we have that channel should we want to use it in the future.

Q161 Lord Strasburger: Would you agree that equipment interference is one of the most technically complex and risky activities that we are looking at in this Bill, and do you think there is a case for having some sort of technical oversight as to what you are being asked to do from a third party, as well as having judicial oversight?

Jonathan Grayling: In the Bill, there is a mechanism to refer to the Technical Advisory Board, and we would expect that Technical Advisory Board to provide that independent oversight. Because of the additional obligations in the Bill, there should be a review of the TAB to ensure that it is structured appropriately and has the appropriate individuals around the table with the appropriate knowledge. That is necessary.

Lord Strasburger: These are very specific skills, are they not?

Jonathan Grayling: They are.

The Chairman: Thank you very much indeed. We have now come to the end of the formal session.