PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

INVESTIGATORY POWERS BILL

Second Sitting

Thursday 24 March 2016

(Afternoon)

CONTENTS

PUBLISHED BY AUTHORITY OF THE HOUSE OF COMMONS
LONDON – THE STATIONERY OFFICE LIMITED

PBC (Bill 143) 2015 - 2016

No proofs can be supplied. Corrigenda slips may be published with Bound Volume editions. Corrigenda that Members suggest should be clearly marked in a copy of the report—not telephoned—and must be received in the Editor's Room, House of Commons,

not later than

Monday 28 March 2016

STRICT ADHERENCE TO THIS ARRANGEMENT WILL GREATLY FACILITATE THE PROMPT PUBLICATION OF THE BOUND VOLUMES OF PROCEEDINGS IN GENERAL COMMITTEES

eThe Committee consisted of the following Members:

Chairs: Nadine Dorries, Albert Owen, †Mr Charles Walker

† Atkins, Victoria *(Louth and Horncastle)* (Con)
† Buckland, Robert *(Solicitor General)*
† Cherry, Joanna *(Edinburgh South West)* (SNP)
† Davies, Byron *(Gower)* (Con)
† Fernandes, Suella *(Fareham)* (Con)
† Frazer, Lucy *(South East Cambridgeshire)* (Con)
† Hayes, Mr John *(Minister for Security)*
† Hayman, Sue *(Workington)* (Lab)
† Hoare, Simon *(North Dorset)* (Con)
Kinnock, Stephen *(Aberavon)* (Lab)
† Kirby, Simon *(Brighton, Kemptown)* (Con)
† Kyle, Peter *(Hove)* (Lab)
† Matheson, Christian *(City of Chester)* (Lab)
† Newlands, Gavin *(Paisley and Renfrewshire North)* (SNP)
† Starmer, Keir *(Holborn and St Pancras)* (Lab)
† Stephenson, Andrew *(Pendle)* (Con)
† Stevens, Jo *(Cardiff Central)* (Lab)
† Warman, Matt *(Boston and Skegness)* (Con)

Glenn McKee, *Committee Clerk*

† attended the Committee

Public Bill Committee

Thursday 24 March 2016

(Afternoon)

[Mr Charles Walker *in the Chair*]

Investigatory Powers Bill

Examination of Witnesses

Alan Wardle and Ray McClure gave evidence.

2 pm

Q77 The Chair: Welcome to the afternoon session. We will now hear oral evidence from the National Society for the Prevention of Cruelty to Children and Mr Ray McClure. We have half an hour for this session. Could the witnesses briefly introduce themselves?

Alan Wardle: I am Alan Wardle. I am head of policy and public affairs at the NSPCC.

Ray McClure: I am Ray McClure. I am the uncle of Lee Rigby, the fusilier who was brutally murdered on the streets of London. I am the eldest brother of his father.

Q78 Peter Kyle (Hove) (Lab): Thank you both for appearing today; it is good to see you.

Mr McClure, could I start with you? We have been talking about the prevention of terrorism to date, but from your perspective this is about crime prevention. Perhaps you could say a few words about that and the measures in the Bill that would benefit crime prevention from your perspective.

Ray McClure: The forces of law and order and security need information in order to prevent crime. Surveillance is a necessary part of crime prevention. You go down the high street or go into shops and you are on CCTV cameras all the time. That is surveillance. The public know what it is for: to prevent crime and to gather information in order to prosecute those who are guilty of committing crime.

This whole thing to date is also about making sure that the forces of law and order—the police and the security forces—have the means of gathering the information that they need in order to prevent crime, be it on the internet or terrorism, as well as being able to gather the evidence in order to prosecute people who are guilty of crime.

Modern society works by having rules that are understood and agreed, and by having those rules policed and enforced. Without those rules and laws in place, we are living in anarchy.

Q79 Peter Kyle: Thank you. Mr Wardle, do you want to give the NSPCC's position?

Alan Wardle: I am happy to. As you would expect, our interest is less to do with the counter-terrorism aspects and more to do with the investigation and prosecution of specific crimes against children. We know, and the Committee will know as well, that the police's ability to investigate and prosecute some of the high-profile crimes we have seen in recent years—online grooming of children and the number of people who are viewing illegal images of children online, which has grown exponentially—is increasingly dependent on communications data. I think it is vital that this Bill ensures that the police have the powers and capabilities to continue to do that.

Q80 Peter Kyle: So from your perspective—and this is from reading the evidence from the NSPCC—this is not just about collecting data; it is about sharing data and intelligence in a joined-up way between the services. Is that correct?

Alan Wardle: It is about collecting data so that, as and when the police need to investigate, there is a dataset that they can specifically and forensically look into to investigate. So data sharing is part of it, but not all of it. Say a child is being groomed online and you are trying to establish where that child was met by someone who has groomed them. Did they actually meet in real life for contact abuse? In the case of a child being trafficked across the country, was a hotel booked? Was a car booked? It is about being able to piece that information together. So traditional policing methods—being able to use the internet and the data that are available from people's online activities to identify people and prosecute them—is the main concern, but the sharing of data, where relevant, is also relevant.

Q81 Peter Kyle: We have seen delays of sometimes 12 months in gathering and processing evidence, insufficient training in the collection of digital evidence—all things you have cited in your evidence—and a lack of awareness of the legal processes to access communications data. Bearing those things in mind, the new powers, even if we had them, could not really be used effectively unless there was the right training in the first place.

Alan Wardle: Absolutely. This is not a silver bullet; it is another tool that the police need in their armoury to help them deal with these kinds of crimes. Equally important is that local police forces particularly have the forensic capability to analyse a mobile phone or computer, and the technical tools and skilled officers to be able to do that.

Being able to access the data is one part of it, but not all of it. The kind of tools that we see at the National Crime Agency and the Child Exploitation and Online Protection Centre are very helpful, but the issue is the extent to which that expertise and those technical tools are disseminated throughout the entire police force across the UK. I would argue that communications data was only ever going to be part of the answer—an important part, obviously.

The Chair: We clearly have two excellent witnesses here, and I am sure that many colleagues will want to ask questions. Who is trying to catch my eye? Would Mr Matheson like to ask a question?

Q82 Christian Matheson (City of Chester) (Lab): I remind the Committee that Mr McClure is known to me, as he is my constituent.

Good afternoon, Mr McClure. The case of your nephew obviously involved a criminal offence and was clearly terrorist-related. There have been suggestions, and we have heard evidence as a Committee, that the

failure was not necessarily one of electronic intelligence, but of human intelligence and a lack of resources, because the security services were already aware of the then suspects—the people convicted of your nephew's murder. How do you react to that?

Ray McClure: It is a bit of both, to be honest. The report by the Government into Lee's murder, "Report on the intelligence relating to the murder of Fusilier Lee Rigby", highlighted failings in the intelligence services and their processes. I do not know personally whether the recommendations have all been implemented, but I have got to assume that they have been, because they were taken very seriously.

Also, the report highlighted other major failings. The ones that caused me the greatest concern were those where the warrants issued by the UK Government were not complied with by American internet companies. *[Interruption.]* Sorry, I am going to pick up my notes. The report made it absolutely clear that the attack by the two murderers of Lee was planned on the internet; they made contact with people on the internet. Yes, opportunities were missed, but internet service providers failed to review any suspicious contacts and they did not obey UK warrants—they went out of their way to obstruct UK warrant providers.

Paragraph 401 says

"some overseas CSPs do not comply with UK RIPA warrants, as they do not consider themselves bound by UK legislation."

That is a failure not of the security services, but of those other people—the internet service providers. Paragraph 457 says:

"The number of different forms of communication now available presents the Agencies with significant challenges in terms of their ability to detect and prevent terrorist threats".

If the internet companies are not co-operating with the intelligence services, there is a big hole there—a big gap that needs to be plugged.

"CSPs based in the US have, for the most part, refused to recognise UK legislation requiring them to provide the content of communications on their networks: they do not consider themselves to be bound by the legal obligations set out in RIPA"—

warrants, etc.

To me, this is a big hole—a big issue. Being somebody from an IT background, I was horrified at some of the stuff I was reading. These companies—Apple, Facebook, Google, Microsoft, Twitter, etc.—are companies that we grew to respect, but the actions that they are undertaking now in not supporting the security and intelligence services, the forces of law and order, to prevent crimes like what happened to Lee, leave a big hole that has to be plugged.

Q83 Christian Matheson: You talk about the lack of co-operation from some of these large corporations based outside the UK. When considering your own investigations and inquiries surrounding the murder of your nephew, have you seen any evidence that that is quite a common trait?

Ray McClure: That is a good question. Yes, I have. I can give two very clear examples. One example is Microsoft, which has been fighting a warrant issued by the US Government to gain access to a drug dealer's emails. It claims that, because the emails are not held on US territory, the US Government cannot have access to them. The emails are actually held in the cloud, and their physical location is in Ireland. Microsoft claims that the emails are a customer's personal documents and that, because they are outside the US's jurisdiction, the US Government and US law-enforcement agencies cannot access them.

That raises a big question mark. Today, when you send an email, you do not know where the physical data will be held—it is held somewhere in the cloud, but you do not know where. That creates a problem for all security and law-enforcement forces. Where does the jurisdiction lie for gaining access to that data? It is a black hole. It is wrong. Microsoft's actions are protecting the drug dealer, not helping law enforcement.

The biggest concern right now—it is a very hot topic—is Apple's stance over the San Bernardino terrorist. He killed 14 people, yet Apple refuses to co-operate with the FBI and allow it to access the data on his iPhone, which might help the police identify his accomplices. That is protecting terrorists, not helping law and order. Quite frankly, I am at a loss as to why the IT companies are so opposed and why they are fighting law and order as they are doing. It is wrong.

Q84 Christian Matheson: Looking at the specific provisions in the Bill, as far as you have been able to check them, are you satisfied that your concerns have been addressed, or was there something else that you were specifically looking for?

Ray McClure: I do not believe that this Bill is adding new powers to the police and the security forces; I think that it is clarifying the existing powers and bringing them together. It makes it a lot clearer where responsibility lies in obtaining warrants and what the powers are. I think that bringing that clarity is a major step forward. Yes, I am happy, and I urge you all to support the Bill. My only concern—it is a personal concern—is that, frankly, I would prefer warrants to be authorised by the judiciary, not by politicians, such as the Home Secretary, but that is my personal opinion; it is down to you guys to make the laws.

Can I make one other point about Apple and Microsoft? These companies are building solutions that we use every day. Let us be honest: these phones that we use today are brilliant, with the address book and everything else. But to make that a no-go area for law enforcement is wrong. There should be no such thing as a no-go area for law enforcement. If you cannot enforce the law, you have a situation in which you are protecting evil, and when you protect evil, evil will thrive, and that is wrong.

The Chair: Thank you, Mr McClure. We have so many colleagues who want to ask you questions.

Ray McClure: Sorry, Sir.

The Chair: No, you are a very strong witness. Mr Buckland.

Q85 The Solicitor General (Robert Buckland): Thank you, Mr Walker; it is a pleasure to serve under your chairmanship. Mr McClure, you have made some powerful points, so thank you very much indeed for giving your perspective on the IT, and as a bereaved relative. We all share your grief and anger about the atrocity.

[The Solicitor General]

Mr Wardle, I want to ask you about internet connection records, the new potential powers within the Bill and the purposes for which those records could be retained by an internet service provider. We know now that, as a result of the Joint Committee's recommendations, there are four purposes for which those records could be retained for potential examination by the authorities. I think that they are very clearly set out: for the purposes of identifying who sent a communication; to establish what services either a suspect or a potential victim has been using; to establish whether or not a known suspect has been indulging in online criminality; and finally—the additional one—to identify services that a suspect has accessed, which could assist an investigation. If there was a narrowing of those purposes, what effect do you think that would have upon the authorities' ability to investigate child abuse and related offences?

Alan Wardle: As I understand it, the previous draft Bill had a narrowing in the fourth one, and I appeared before the Joint Committee before Christmas to argue against that narrowing. I cannot remember the exact wording, but it was essentially where illegal activity was happening.

Again, I go back to the example of the grooming case I mentioned earlier. Grooming, by its very definition, takes place over a period of time. There are certain activities that you would want to investigate that are perfectly legal. Say a child has been trafficked across the country. Someone has hired a car, taken it from A to B and dropped it off, and they have gone on to the Travelodge website to book a hotel room. All of those are perfectly legitimate activities, but those activities—as part of a wider investigation—would be able to show the police that that person trafficked that child from A to B and that those activities took place. Clearly more would be needed, but the narrowing that was there before would, we believe, have unduly restricted the police's ability to investigate those kind of crimes.

Q86 Joanna Cherry (Edinburgh South West) (SNP): May I ask you some questions about internet connection records? Can you confirm that you have read the operational case for internet connection records referring to the case of Amy?

Alan Wardle: I do not think I have read that.

Joanna Cherry: It is about a missing child.

Alan Wardle: Oh yes, I know it.

Q87 Joanna Cherry: Would you agree with me that if a child goes missing, the first thing you want to do is to find out what social media or chat sites the child has been on?

Alan Wardle: Whether that is the first thing you want to do, it is certainly—

Joanna Cherry: It would be a priority.

Alan Wardle: That would be something that the police would want to investigate pretty quickly.

Q88 Joanna Cherry: Is not the easiest way to do that to ask their friends?

Alan Wardle: It could well be, depending on what has happened. In an ideal world, the child would keep all the evidence themselves and it would all be freely available in terms of the content, but things are deleted and friends are asked to keep quiet and so on, so it is not always necessarily available. If the child has been groomed, they may have been taken by someone they think is their boyfriend, away from their dreadful parents—they are running away.

Q89 Joanna Cherry: Sometimes the child will take their phone with them and it will be switched off and be no use to us, but other times they will leave their phone behind and we can get into the phone and see which social media sites they have been on. Is that right?

Alan Wardle: I am not a police officer, but yes, I presume so.

Q90 Joanna Cherry: Equally, if there is a computer at home, the police can access the computer with the parents' permission and see what social media sites the child has been on?

Alan Wardle: Yes, but three quarters of 12 to 15-year-olds have a mobile phone or tablet, so it is rarely the computer on the dining room table any more.

Q91 Joanna Cherry: If we assume that the computer and the phone are not available, you could go to friends or siblings and find out what social media the child commonly uses. If, for example, the child commonly uses Facebook, the friend will be able to tell you what the child's username is.

Alan Wardle: Well, the child's username would be their real name because Facebook has a real name policy.

Q92 Joanna Cherry: Indeed, and they will know what their friends' names are. I do not really know how Bebo works, because I am too old, but if it is not a known name on Bebo, you are still able to get the username from the child's friends.

Alan Wardle: I would imagine so, yes.

Q93 Joanna Cherry: Does it not really boil down to this: wherever you get the information from—whether it is mum or dad or, more likely, mates at school—you have to go to Bebo or Facebook and ask for their help?

Alan Wardle: The social media companies clearly have a huge part to play in this as well. We challenge them regularly on all aspects of how they keep children safe online. What is important when the police are investigating such crimes is that they have every tool available to them that can legitimately be made available. Some will be traditional policing methods, such as asking their friends and knocking on doors, and some may be much more technical aspects, such as internet connection records.

Q94 Joanna Cherry: But would you agree with me that what is important is to have effective tools?

Alan Wardle: Absolutely. One of the things we have challenged the internet companies on is that if those tools are available, they should be widely available. A good example is what is called PhotoDNA, which basically means that illegal images of children are hashed and can be removed across the internet. That is a really

positive development. That technology was developed by Microsoft, but shared across all the big companies, which is a really positive thing.

We know that there are other technologies—anti-grooming technologies, for instance—that have been created, but have not been shared in that way. I think that there is an obligation on the companies—your Apples, your Facebooks and your Microsofts—to ensure that these kind of tools, with no real commercial gain to be made from them, should be freely available across the industry.

Q95 Joanna Cherry: If we just go back to the example that I was pursuing, about the missing child, I think you agreed with me that it is important to have effective tools. Is it your understanding that all the internet connection record will tell you is what the missing child connected to? It will not tell you what the missing child did once they were connected.

Alan Wardle: No. That is the issue to do with content. Again, it could well be that that is part of a wider picture.

Q96 Joanna Cherry: An internet connection record will only tell you to which service the child was connected, not whom they spoke with, nor what the content of their speaking was—

Alan Wardle: Not necessarily.

Q97 Joanna Cherry: Whereas, if you go to the child's friend and get the child's username on the social media site, you will be able to get that information as to content.

Ray McClure: You would still need the child's password to access the data.

Alan Wardle: That is not enough in and of itself. Yes, do you have the password? How would you get into it?

Q98 Joanna Cherry: You will not get passwords from an ICR?

Alan Wardle: No.

Q99 Suella Fernandes (Fareham) (Con): There has been a description of Tor as a facility that allows digital abuse of anonymous online activism. It is linked to encrypted information. I want you to say a bit about what effect encryption has on some of the work that you are involved with?

Alan Wardle: A lot of the activity that we take for granted online—shopping, banking and all the rest of it—could not be done without encryption, but of course, as with all these tools, encryption can be used for bad purposes by bad people. Similarly, with services like Tor and Freenet—the dark web—in the cases that we are concerned with, you get your most highly committed and dangerous offenders, quite often, particularly sharing very explicit images or videos of children being abused. Those services enable them to hide there. The police do the best they can, but, again, for a lot of that they will be dependent on traditional undercover techniques.

I think there is a question that is—I say this respectfully—beyond this Committee's remit and beyond many of our remits. The direction of travel generally is that we are seeing greater moves to encrypt data as a matter of course, with things like Google Chrome browsers and so on. With browsers such as that, internet service providers cannot put in place the kind of protections they have, so they do not know what is going on there. That is a direction of travel and something that is worrying. It is clearly a global issue, but the police not being able to track what is going on due to increasing levels of encryption is a worry.

Q100 Victoria Atkins (Louth and Horncastle) (Con): Just to pick up on the point made by the hon. and learned Member for Edinburgh South West about the missing child, is it right that, sadly, the victims of sex grooming rings do not surround themselves with friends and parents, because one of the tools that the groomers use is to isolate the victims, so that they have no one they can turn to in their hour of need?

Alan Wardle: That can be true. They can even turn the child against their family and friends as well.

Q101 Victoria Atkins: So in those circumstances, as you have said, the police need every tool that they can get to help those very vulnerable young children.

Alan Wardle: Absolutely. Again, as I have said, the issue of grooming is often about a period of time and establishing patterns of behaviour. Being able to gather evidence from a range of sources is really important.

Q102 Lucy Frazer (South East Cambridgeshire) (Con): Following on from that, in your work in the NSPCC, do you always see a willingness for children to open up and to tell people in a position of authority personal facts about themselves and their friends, or can it be quite difficult to coax out information about children who are friendly with the vulnerable?

Alan Wardle: It will depend. Generally, it takes quite a lot for a child to come forward and disclose. In recent years, we have seen a huge increase in the number of children who are reporting sexual abuse generally. It is going up across the UK, and was up by about a third last year. A large part of that is because of a greater willingness of children to come forward and talk about the abuse that has happened to them, but we know that it can take decades for people to come forward and talk about abuse.

What we are talking about, particularly sexual abuse, is a very personal thing, so the idea that a 15-year-old who is being groomed will just walk straight into a police station and start disclosing all these very personal things is generally not quite how it works.

Q103 Lucy Frazer: I was also thinking about the case of missing children. If we rely only on their friends and those friends are not willing to disclose personal details, names and the social media sites that their friend is on, do you think there might be a delay in an investigation?

Alan Wardle: There could be, and it depends on the facts of the case. I will return to the main point. As I said before, the police need a range of tools. They will need some very traditional knocking-on-door tools, and they may need a range of technical tools to help identify a child in that situation.

Q104 Lucy Frazer: So it is a combination of tools that will keep children most safe?

Alan Wardle: Yes.

Q105 Andrew Stephenson (Pendle) (Con): I thought you made a compelling case in your evidence to the Joint Committee; I was not a member of that Committee, but I have watched it back on video. You made a compelling case for why timeliness is very important when a child is threatening to commit suicide—basically having to breach that child's confidence to ensure that the police can intervene. The expression you used was about literally having to cut children down at times.

Could you say anything more to this Committee about that? Some members of this Committee sat on the Joint Committee, but others will not have heard that evidence. Could you say more about the need for rapid intervention to save children's lives?

Alan Wardle: The NSPCC runs ChildLine, a service that people will know. About three quarters of children who contact us do so online, rather than through the traditional telephone service. We have a very high level of confidentiality, but in an average of 10 cases a day we have to breach a child's confidence because their life is in imminent danger. In 60% of those cases the child is actively suicidal; on average there are six cases a day where we have to contact the emergency services to protect a child whose life is in immediate danger because they are suicidal.

On the capacity for the police to be able to find where that child is, if they are on a mobile phone, for instance, an IP address would not cut it. We have cases where children who have tried to kill themselves are literally saved because of the 24/7 service that we run, and the police's ability to be able to rescue actively suicidal children in real time is very important.

Q106 Simon Hoare (North Dorset) (Con): This question is to both of you. Is there anything that is not in the Bill that you would like to have seen, or maybe still see, in the Bill?

Ray McClure: It is not really relevant to the Bill in question, but you have to find some means of punishing companies that do not comply with warrants issued, and it has to be a heavy punishment. Right now, without having legally enforceable warrants, there is no law enforcement and no justice.

Alan Wardle: I do not think it is necessarily about what is not in the Bill, but I reiterate the point I made earlier: these internet connection records are only part of the solution. There is a whole range of things in terms of keeping children safe online, particularly on the capacity of the police to respond to that and to be able to have the right tools to investigate, prosecute and convict criminals. These tools are very important, but there is a much wider piece about how the police can use all the powers available to them to help keep children safe.

The Chair: Mr Kyle, a 10-second question and a five-second answer.

Peter Kyle: Mr Hoare has just asked my question, so I am a happy man.

The Chair: That brings us to the end of this session. May I thank our witnesses, who gave extremely strong performances? I know that being a witness before a Committee is very nerve-wracking, but you both executed your role fantastically, so thank you very much indeed. It was very kind of you to come before us today.

Examination of Witness

Mark Hughes gave evidence.

2.30 pm

Q107 The Chair: Good afternoon, Mr Hughes. Thank you for coming here before us today. For the record, I know Mr Hughes outside this place. I had no idea that I was going to be here this afternoon, but here I am and here you are. Would you like, for the benefit of my colleagues, to introduce yourself quickly? There will be lots of questions.

Simon Hoare: Just for the record, I also know Mr Hughes, though I cannot remember how—I am having a senior moment.

Mark Hughes: We will work it out afterwards. I am happy to get to know everyone else on the Committee. I am the CEO of BT security, and I have responsibility for all the matters that relate to the Investigatory Powers Bill in BT.

The Chair: Excellent.

Q108 Keir Starmer (Holborn and St Pancras) (Lab): We have a definition in the Bill, as I am sure you know, of an internet connection record. What is recorded by BT or any other service provider if I book a train ticket on my mobile phone? What comes up on your record?

Mark Hughes: I would like to answer that question looking more at the Bill itself, and then come back to your question. There are clearly quite specific provisions in the Bill on what we are there to collect.

Q109 Keir Starmer: We have a definition—I would have copied it to you, but you probably have it there—in clause 54(6). You probably know it backwards.

Mark Hughes: Some examples of what we are talking about—I am sorry to be technical, but it is important that I refer to some technical matters—are the customer line reference number, which we perhaps know in common parlance as the account number, and the source and destination host IP addresses. The port to and from it provides content that we have to collect. There are also mass data sets. The Bill is quite clear about what we are there to collect.

On your specific question about a service where you are booking a train journey, we retain various components of the types of data that I just spoke about. It would be things such as source and destination IP addresses and the handset you used, which you mentioned specifically. The IMEI, for example, is another piece of data that associates you to that handset.

Q110 Keir Starmer: If I went to the Trainline website, for example, although it would not come up as Trainline, could you work out that I had been using that website to book my ticket?

Mark Hughes: No, not at the moment. That is not how it currently works. As I understand it, there are four purposes of internet connection records in the Bill, which are to link an IP address to a person or apparatus; to identify the comms service a person is using; to identify where a person is accessing illegal material; and finally, to identify the internet services a person is using, which is pertinent to your question.

What the Bill proposes we are to collect—some of which, by the way, is drawn from data sets that we collect for normal business purposes—may be used to constitute an internet connection record, which would then satisfy those purposes. It is not something we currently retain. The Bill is clear about the ingredients of an internet connection record and its purpose. At the moment, we are still working out with the Home Office exactly how we would compile those pieces of information to create internet connection records and find out which website someone was visiting.

Q111 Keir Starmer: I am sure all that is right, but I am still not sure that I have an answer. If I book a ticket now on the Trainline website, would it come up on your record that I had done it?

Mark Hughes: It is not something that we currently collect and retain.

Q112 Keir Starmer: Not currently, but when the Bill is law.

Mark Hughes: Yes, the Bill quite clearly states the purpose about identifying the internet service that the person is using—

Q113 Keir Starmer: So it would come up?

Mark Hughes: One of the purposes is that we would then be under notice to retain and create that record, which we do not currently do at the moment.

Q114 Keir Starmer: So if the Bill becomes law and I then book a ticket on the Trainline website, you would record it?

Mark Hughes: Under the Bill, once we had been through the consultation process and notice was given, that would be one of the purposes.

Q115 Keir Starmer: Sorry—I probably should have said that I am not that interested in the process at the moment. I understand the process and of course all the proper processes would have to be followed. I am just interested in what you would get before the process starts.

May I try a different question? If I go through the tube using electronic means of payment, would that—if the Bill becomes law and assuming that all the processes are followed—show up on my record?

Mark Hughes: That would not be information that we had access to. It is not our information; you would have to ask TfL that.

Q116 Keir Starmer: What about a feature that I have on my phone called Onefootball? Unbeknown to everybody else, my phone asks for the football scores all the time. What would show up on my record if the Bill became law and assuming that all the processes were followed and all the rest of it?

Mark Hughes: Again, it depends. There is some technical detail underneath here in respect of how that particular service provided by that service provider, Onefootball, polls out and how it would use the services that underlie that—that is, the services that we provide. That would obviously then be subject to the process that would then end up with an internet connection record, if that were appropriate in that case. Or it might be that you would have to go to that service provider to gain information.

Q117 Keir Starmer: But if it were you, would it show that I had been asking for football results all afternoon?

Mark Hughes: If there was an internet connection record under the definition of the Bill, one of the purposes of which would be to identify which internet services you had been using, yes, we would then retain that and disclose it under the appropriate instrument.

Q118 Keir Starmer: And if I went to the website of *The Guardian* and clicked on "Brussels attack" and then clicked on "Another bomb", what would be on your records—assuming that the Bill becomes law, that all the processes are complied with and that there is a proper purpose? I am making all those assumptions. I just want to know what would be on the record.

Mark Hughes: We have obviously been spending a lot of time in consultation with the Home Office. There are varying degrees of capability that the Home Office wants. There is a technical element to how far one goes in terms of the amount of data—there is a trade-off between the amount of data that you collect, retain and then disclose. As the Bill stands, that would also constitute an internet service that someone was using so that would be something on the Bill that we would retain.

Keir Starmer: Thank you.

Q119 Joanna Cherry: At the Joint Committee, Mr Hughes, you said that BT had never collected internet connection records before, that you would have to deploy new equipment to comply with the legislation and that that would come at a cost. That is correct, is it not?

Mark Hughes: That is correct, yes.

Q120 Joanna Cherry: I understand from your answers to Keir that you are still working with the Home Office to agree the precise specification of what an ICR is. Is that right?

Mark Hughes: That is right, yes.

Q121 Joanna Cherry: Are we to understand, then, that you have not as yet reached agreement with the Home Office about the specification of an ICR?

Mark Hughes: No. It is a work in progress. This is quite a truncated time frame, as you know. I characterise a lot of things that we are doing at the moment as "in parallel" as opposed to "in series".

Where we are at the moment is that there has been extensive consultation with the Home Office around this. There are a number of different technical approaches to how you take those component parts that then constitute themselves as an internet connection record—for example, things like the rate of sampling that you use inside the networks. Of course, it depends on the type of service that we are talking about; there are technical differences between how those services and that information are then put together to create the internet connection record. That has a big difference in terms of the associated cost.

Q122 Joanna Cherry: That is what I want to come on to. The Home Office has mentioned a figure of £170 million. Can you give us any indication of how much of that money British Telecom would need to build a system?

Mark Hughes: There is a spectrum. If the Home Office wanted us to collect everything and carry out a very high rate of sampling, meaning that a lot of information would potentially be available, BT—and EE; we recently bought EE, as you may know—would take the lion's share of that figure alone, just in terms of our services.

However, we are in very frequent dialogue. Only in the last couple of days, we have been talking to the Home Office about the technical challenges associated with the trade-off between how much it will cost and how much data will be available. Clearly, if there is a different view in terms of the amount of data required, the cost may well be appropriate for the rest of the industry. It is difficult for me to comment on other operators.

Q123 Joanna Cherry: We have covered potential costs of building the system. Can you give us a timescale?

Mark Hughes: Again, that is down to the detailed, technical implementation and testing to ensure that it would work properly. Some of the data sets that make up the ingredients of an internet connection record are something that we do retain for business purposes already—not necessarily for the length of time they are talking about—so depending again on the final technical solution we came at, and at what services it is targeted, it could take a few months and up to a year-plus to get a solution in place.

Q124 Joanna Cherry: When you say a year-plus, how much on top of a year?

Mark Hughes: Again, depending on exactly what it is that we agree on with the Home Office that it wants, I think it is reasonable to suggest that we would have a service in place in a year.

Q125 Joanna Cherry: Are you aware of what has happened in Denmark regarding the collection of internet connection records?

Mark Hughes: I am, yes.

Q126 Joanna Cherry: On 17 March, the Danish Minister of Justice informed the Danish Parliament that the plans for a new internet connection records scheme had been put on hold. The reason given for the policy change was the substantial cost of ICR collection—the economic burden would be too high for the Danish telecoms industry. Were you aware of that?

Mark Hughes: I am aware of that. Under the proposals in the Bill—the Home Secretary has made reference to it—we would recover our costs from the Home Office, as we have done under existing legislation. We would like to see clearly articulated on the face of the Bill that 100% of our costs are to be recovered. That is very different from the Denmark situation. In Denmark, that is not the case; the burden is placed on the telecoms operators.

It is difficult for me to comment precisely on the Danish telecom operators because I am not one of them, but specifically here, as far as the UK is concerned, the proposed regime is more sensible as long as it is clear that we will recover 100% of our costs. We think it is important that that is on the face of the Bill—not just for the reason we said about Denmark, but also because more broadly in itself it provides a proportionality check, so you would not spend a huge amount of money to achieve little effect. If it is clear how much the public purse will have to bear of that, we think that in itself creates a proportionality check in terms of what activity is proposed.

Q127 Joanna Cherry: Do you agree that we cannot compare what is proposed in the Bill with what was proposed in Denmark until you have got an agreed specification with the Home Office?

Mark Hughes: A pamphlet has been issued and we have been in discussion with the Home Office as recently as the last couple of days about this. More clarity is required, but broadly speaking there is a definition in the Bill, there are purposes in the Bill and we understand that there are options technically around it. We have been working that through with them, but yes we would like clarity as soon as we can.

Q128 The Minister for Security (Mr John Hayes): Thank you, Mr Hughes, for coming, and thank you also for acknowledging the extent of the consultation with which you have been engaged with the Home Office. As a result of that, you will know that the codes of practice published at the time of the Bill reflect some of the arguments you have advanced previously and clarify some requirements.

Today you emphasised that as we move forward there will be ongoing discussion. How important do you therefore think it is to avoid rigidity by putting more on the face of the Bill rather than including that in codes of practice and in the ongoing discussions you described?

Mark Hughes: It is very important that we have words and definitions on the face of the Bill to deal with the really substantive points as far as this type of legislation is concerned—namely the level of intrusiveness, which is clearly where definitions help. A definition is only really a way of helping to establish the level of intrusiveness of the power that is being put in place.

There are needs to have something. One need, which I have said, is about ensuring that there is clarity around 100% cost recovery, for example. There is definitely a need for that and with 268 pages there is quite a lot in there. However, we also recognise that as technology changes—our world is an ever-changing one as we know, and that is the case specifically in our industry—there is need for flexibility of a discussion point around how consultation happens and how that manifests itself in a legal instrument for us to retain and disclose either content or other types of communication data.

It is a difficult balance to be had. I think there is a lot at the moment in the Bill that is very useful. There are purpose limitations, for example, which are very useful for us, as are, as I said already, the definitions.

The other point is that there does need to be flexibility in future about understanding how the new codes of practice will be formulated based on what was required, and the Bill is clear that the correct oversight is in place. That is a difference from the extant legislation. The consultation process is different from others there have been in the past, and we welcome that.

Q129 Mr Hayes: Presumably you also welcome the right to review a technical capability notice and the commitment that there will be further discussion with you before you are obliged to meet obligations.

Mark Hughes: Yes, indeed, and not only that, but there is now on the face of the Bill a right of appeal to the Home Secretary if a notice is issued to us and we disagree with it. That has not existed in the past. In the past, under other legislation, we have had occasion to make representation, but it is much clearer in this Bill than it has been in the past.

Q130 Christian Matheson: Under the terms of the Bill, you are being asked to collect a large amount of data, some of which will be quite personal and some private. How confident are you of BT's capability in terms of maintaining the security of those data from hacking or theft, particularly bearing in mind the fact that other communications service providers have been hacked into? When you consider the rest of the industry more broadly—without naming names—do you think BT is in a stronger position than other CSPs to maintain security against hacking or theft where there might be vulnerabilities elsewhere?

Mark Hughes: The security of any data we hold and retain is clearly a matter that we take extremely seriously. That is of the utmost seriousness for our organisation for any type of data. The type of data that the Bill refers to specifically is, though, perhaps different from other types of data that need to be interfacing the public on a bigger scale, for example. This is not that type of data; it is going to be restricted and allowed to be viewed by only very few individuals who have the correct authority to be able to get to the data when they need to.

The level of security applied to this type of data is clearly factored into the type of data that is being retained, so we have to put very significant security measures around it to ensure that the access is controlled properly and that the data are very secure when stored. That absolutely has to be factored into the cost and the way we operate. It is not something new. We are currently subject to laws and regulations under which we have to make sensitive data available, so we are used to doing it, but that clearly has to be factor in for, for example, some of the new datasets we are potentially going to be asked to retain under the Bill.

Q131 Matt Warman (Boston and Skegness) (Con): On the Joint Committee on the draft Bill and on the Science and Technology Committee, we heard CSPs talking about the level of engagement they have had from the Home Office, and we have heard from the Home Office that that has increased recently. That seems to tally with what you are saying. Could you give us a sense of the scale and extent of that engagement, and some reassurance that, in this fast-moving world, you are confident that the relationship is such that that engagement would be there in future as well, rather than it just being about getting the Bill to this stage?

Mark Hughes: We have had extensive periods of consultation and meetings on a very frequent basis. The Home Secretary has invited many of us representatives of the CSP community to meetings with her on two occasions before this, as well as to many working-level meetings with various Home Office officials. We discussed the technical, legal and procedural points about the proposed legislation as well, which is markedly different from how things have been before.

On the point about the future, which is important here, the Bill itself clearly specifies and puts in place a regime whereby consultation is enshrined in the legislation through the consultation process that has to happen before a notice is issued and, indeed, because the reconstituted technical advisory board can be called to come together at any time. That power did not exist in the past. The consultation is in a better place and I think that the Bill itself will help to ensure that that continues in future, because it will be a point of law.

Q132 Peter Kyle: Is everything in the Bill technically deliverable?

Mark Hughes: There is nothing that we have yet come across that we think is technically not deliverable. However, I will caveat that by saying that we provide many different services. There are different service providers that do different types of things and operate their communications networks differently from us. I can only really comment on BT and our networks, both mobile and fixed, but from where we are coming from it is—

Q133 Peter Kyle: So through technology that is already in existence and already within your grasp as a company, everything in the Bill is within the bounds of deliverability.

Mark Hughes: What I would say is that, as I said at the beginning, the things in the Bill that we need to retain are what bits we can do technically. We have not yet gone through in detail how we constitute some of that information, because we have not yet done it. I cannot comment on something that we have not done yet, but on the face of it, it does not look unfeasible.

Q134 Peter Kyle: To follow up briefly on Mr Matheson's question about security, I hear your answer, which is quite broad. I will rephrase the question in this way: would existing BT customers expect a different level of security protection for their data once the Bill is enabled and passed, compared with what they expect and what is at their disposal today?

Mark Hughes: Again, different types of data, depending on the concentration, volume and type of data, require different levels of security. We always assess the risk of that data becoming exposed in a way that it should not, and we assess the security against that clearly.

Q135 Peter Kyle: Are you saying that because the quantity and volume of data being stored will increase and you are storing it for longer, those are two contributing factors that could potentially lead to the weakening of security?

Mark Hughes: No. On the contrary, because that is the case, we will assess it and have to put additional security controls around those data. Again, some of those data sets do not currently exist. In assessing how we would build the storage for those data sets, we would obviously factor in security, and some of the factors would include the volume and type of data, which would lead to the solution that we put in place. That is part of some of the cost estimates that have been worked through in the pamphlet produced by the Home Office.

Q136 Gavin Newlands (Paisley and Renfrewshire North) (SNP): This is a quick follow-up to a question Mr Starmer asked earlier about ICRs as they relate specifically to mobile devices. The example that he gave involved a football app, but let us use Facebook as an example, as it may be of use in investigations. Facebook and apps like it have lots of background processes that generate thousands of ICRs. Is there any way of ascertaining whether an ICR is created manually or automatically by the app?

Mark Hughes: I think there is a principle here. Again, it is enshrined in the Bill to a certain extent, but I make the point now. The organisation that holds the data closest to source is the one that should be subject to the powers. That is the one that should be retaining and having to disclose data under the Bill as it stands. For example, you mentioned Facebook. If Facebook has those data, they are the ones you would have to ask about how they would go about retaining and disclosing it.

Q137 Gavin Newlands: I understand that, but would it be technically possible to understand whether somebody has pressed a button to create that record or whether the app has done it?

Mark Hughes: I would have to look specifically at the details around it. If it generated an internet connection record that was a website visit, for example, that might be something that we retained, but it would be very difficult for me to comment specifically on that without knowing the exact details. It depends on the engineering of the services and networks, but in principle, if Facebook had that data, then they are the ones that should be subject to the law. We are considering whether to propose an amendment to the Home Office on the third party data question, which is the case in point here, and how that should be approached. We think that the principle is that other providers who have that data are the ones who should be subject to it, and that it should be explicit in the Bill.

Q138 Gavin Newlands: So at the moment the Bill is not clear enough on that aspect?

Mark Hughes: It could be clearer, and we are thinking about proposing an amendment specifically to over-the-top providers, making it clear that they are responsible for that.

Q139 Keir Starmer: Can I come back to the question of what constitutes an internet connection record? It is the record that you may be responsible for keeping and passing over, so it is important that you have clarity. I take it from your previous answers that you have said some of it will be data that you are already collecting for your own purposes, and some of it will be other data that you are not currently retaining but will retain as a result of the Act. What are the data you are currently retaining? What is the bit that you keep already?

Mark Hughes: I gave an account number as an example. We obviously know our customers' account numbers, so that is something that we currently have, and we have other types of information, as I went through, which are potentially subject to other pieces of legislation on retaining data. The point about the internet connection record is that it is rather like a series of ingredients, which you have to put together to create the record.

Q140 Keir Starmer: I have got that. The account number is fine. That does not tell you very much; it is just the account number. When someone does something using the account, what else do you keep at the moment?

Mark Hughes: There are other records associated with other types of services that we have.

Q141 Keir Starmer: I am sorry; I am struggling with this. Can you give me an example?

Mark Hughes: A source-destination IP port, for example. That is something that has to be available to allow traffic to route around the internet. That is the type of data that we have.

Keir Starmer: The IP port?

Mark Hughes: The extent to which we collect and retain that at the moment is clearly going to depend on our being clearer about what an internet connection record is through the work of the consultation. That will drive how long we have to hold the source-destination IP.

Q142 Keir Starmer: What data that you do not currently retain or keep will you have to add as an ingredient?

Mark Hughes: As far as I am aware, nothing. At the moment, we have—

Keir Starmer: Nothing?

Mark Hughes: Well, we have information at the moment that we might not retain for a period of time, but which would be commensurate with what the internet connection record is going to be. It is less about the type of data and more about the length of time that we have to retain it. That is the thing that we need to work out through the consultation process. Does that make sense?

Q143 Keir Starmer: Just to clarify, I heard you say earlier that some of the data you keep and some you would have to constitute. Now, you are saying that it is all data you have got; it is just about how long you keep it for.

Mark Hughes: No. Sorry if I have not been clear on that. The ingredients are there in some shape or form. Some stuff we mainly retain for a very brief period. There are elements of the data that we would have to look at very differently if the Bill became law, in terms of the length of time, how we retain them and how we use them to produce the internet connection record. That would be different.

Q144 Keir Starmer: If I were your customer and this Bill were law and I accessed *The Guardian* through you, would you think that one of the ingredients is the page within the home page that I went to? Is that an ingredient that you anticipate that you will have to keep?

Mark Hughes: Sorry, I did not hear the question.

Q145 Keir Starmer: If I go on the *Guardian* website, I can start clicking between different parts of the website for different bits of information. You can go on a hyperlink to different pages. Do you anticipate keeping any of that data in the future if I were your customer?

Mark Hughes: As drafted, the Bill talks about identifying the internet service that a person is using. The extent to which that capability will be required on the face of it is subject, as I mentioned earlier, to some of the technical considerations. For example, for what you are describing, if every single thing you were to click on on that particular website needed to be retained, that would require a lot of information, which we would have to generate from our network. Technically speaking, it would require a lot of sampling of traffic to achieve that.

Q146 Keir Starmer: That is a technical issue, but legally do you think it is within the definition you are working to?

Mark Hughes: Absolutely. I think it is within the definition as it is written in the draft Bill at the moment.

Q147 Lucy Frazer: Following on from Keir's questions, there is a concern about the hackability of the volume of data that we have already got. Have we just heard that you already collect this data, albeit not necessarily in the same form or for the same length of time? Is it all still there for someone who wants to access it immediately?

Mark Hughes: No. Not all of the data is collected. We retain lots of data for business purposes, which we therefore retain and secure proportionately and appropriately for that type of information. As I said, there are things in the Bill that are about us having to generate additional records, based on some of the existing information that we have and other types of information that may be necessary in the future.

Q148 Lucy Frazer: But based on the existing information that you have, it is already there.

Mark Hughes: Some of it is already there. Some of it might not be there in the way in which the Bill describes. Some of it is subject to what the actual code of practice determines we have to collect and for how long we have to collect it. Some of those things are unknown at the moment. Suffice it to say, we have lots of information, some of which could constitute or make up an internet connection record as it stands at the moment. We secure that data, and it is accessible if required for business purposes at the moment.

The Chair: Thank you very much, Mr Hughes. I am sorry we do not have more time.

Mark Hughes: I am happy to submit written evidence post the sitting.

The Chair: Excellent. Colleagues may follow up your evidence with written requests as well.

Examination of Witnesses

Richard Berry, Chris Farrimond and Simon Grunwell gave evidence.

3 pm

The Chair: Colleagues, before we see our next panel, may I say that we need to exercise some extraordinary self-discipline with two of these panels? We have three witnesses coming forward on this occasion, before we go back to a single witness. We then have four witnesses for half an hour. Can I ask Front Benchers particularly for discipline and sharpness in questioning, so they are razor sharp?

Thank you, witnesses: do sit down. Because time is pressing, will you tell us briefly, in no more than 10 words, who you are and whom you represent?

Richard Berry: I am Richard Berry, the assistant chief constable from Gloucestershire and the national policing lead for communications data.

Chris Farrimond: I am Chris Farrimond, from the National Crime Agency. I am the deputy director for intelligence collection.

Simon Grunwell: I am Simon Grunwell from Her Majesty's Revenue and Customs' fraud investigation service.

Q149 Keir Starmer: We are trying to get to the bottom of what an internet connection record means in the Bill. We have the words on the page in front of us. From a practical point of view, should this Bill become law, what do you think is going to be made available to you when you need to get an internet connection record?

Chris Farrimond: We put law enforcement requirements into the Home Office, which we gave quite some detail around—the who, where, when and how of internet connection—and the internet connection record has been defined as a result of that. We believe that what we will get is down to the domain name, so it will give us, for example, *The Guardian* newspaper website, the easyJet website, or thetrainline.com. It will not give us beyond that. If we wanted to go beyond that, we would then have to go to that company with the appropriate authorisation in order to obtain any further details. What we need is to get to the front door. That is what we have been asking for.

Q150 Keir Starmer: Can I just make sure I have understood that? For booking a train ticket or something, I can understand that you need to go to the next level if you want to find out the particulars. If it is *The Guardian* website, what comes up first is a website. You can then click on it if you want to go to national news or international news, and within international news, you could go to Brussels, for example, as many people might have done in the last day or so, so you have gone through a couple of hyperlinks to a different page. Will the fact that you have done that come within what you consider to be an internet connection record? I can see for booking a rail ticket that you would have to go in to get the detail of what ticket, where to and all the rest of it, but when someone clicks through to linked sites on let us say, *The Guardian,* would you expect that to come within the definition of internet connection record?

Chris Farrimond: Our understanding, and what we have been asking for, is just to get us to the front door—the front door that is marked *The Guardian*, at which point, if we needed to go to *The Guardian* newspaper to ask for any further details, we would do that.

Q151 Keir Starmer: On internet connection records, as I have understood it, the purpose of getting the internet connection record in practically all cases is to bridge pretty swiftly into content using other lawful means.

Chris Farrimond: No, I would not agree with that.

Q152 Keir Starmer: What would you use them for?

Richard Berry: From our perspective, the use of the internet connection record would be very similar to that for which we use communications data anyway. That is potentially to identify further lines of inquiry—for example, that communications service that is accessed. It could be for evidence of illegal material, or the use of illicit material, whether that be child abuse imagery or counter-terrorism-related material, but also to provide a seed for further inquiry, such as thetrainline.com for us to establish, for example, where a suspect has travelled to and where they are intending to travel to. It is about an evidential line of inquiry. It could be evidence in itself, but also a seed for further investigation.

Q153 Keir Starmer: But in most cases it would be the seed for further investigation. Would it be rare for it to be an end in itself?

Richard Berry: Indeed, because of its high granularity.

Q154 Keir Starmer: No other country is going down this route to solve the problem of access, which is a growing problem. What are other countries doing if they are not doing internet connection records?

Chris Farrimond: Sorry, I am not convinced that you are correct in that last statement that no other country is going down the same route. I believe Australia has gone down a similar route. Perhaps we need further clarification on that, but my understanding is that Australia has gone down exactly the same route.

Q155 Keir Starmer: Yes, but I think they have backed up a bit. Which other countries, to your knowledge, have a power to access internet connection records in the way proposed in the Bill or a similar way?

Richard Berry: None at this stage. I think there is a common view within the law enforcement community globally that all eyes are very much on the UK to pave the way in this respect. We are aware of the danger of the Danish experience and the difficulty the Danes had with the type of data they collected to achieve the investigative aims, but while the Australians are making steps in that direction, as Chris has highlighted, at this stage it is very much the UK leading the way.

The Chair: Thank you.

Joanna Cherry, if I give you six minutes—I gave Keir six minutes—you will know what you are working with.

Q156 Joanna Cherry: Thank you, Mr Walker.

Mr Farrimond, are you aware that just last week the Danish Minister of Justice informed the Danish Parliament that plans for a new internet connection record scheme have been shelved in Denmark?

Chris Farrimond: Yes, I am.

Q157 Joanna Cherry: Are you aware that the reason given for that was the substantial cost and the economic burden for the Danish telecom industry?

Chris Farrimond: Yes, I am aware of that too.

Q158 Joanna Cherry: I want to change tack slightly and ask you about the police online Crimestoppers website. I am sure everyone agrees that it is a useful service.

Chris Farrimond: Yes.

Q159 Joanna Cherry: I looked at it again this morning and it says that when you fill in their form and say you want to be anonymous, you are guaranteed anonymity. That is correct, isn't it?

Chris Farrimond: Yes, it is.

Q160 Joanna Cherry: But if we pass this Bill, that assurance will no longer be accurate. Isn't that right?

Richard Berry: That is a technical observation, but I think the point is that, in terms of the collection of data and, more importantly, police access to or acquisition of that data, we are looking for stuff that is relevant and useful. So a line of inquiry or a justification for accessing the Crimestoppers website from my perspective could not be justified in terms of the necessity and proportionality tests required for giving that authority.

Q161 Joanna Cherry: If we could reel back a little, if this Bill is passed, the purpose of internet connection records, we have been told, is to have a record of every device's connection to every service. If anyone goes on to the Crimestoppers website and fills out the form, there will be a record of their connection to that service, so it is correct to say that their anonymity is no longer guaranteed. Is that not absolutely right?

Chris Farrimond: Where is that different from Crimestoppers? If someone phones in, they are guaranteed anonymity, but if we wanted to we could easily find out who made that call. We don't because we guarantee anonymity. If we didn't, no one would phone the number any more.

Q162 Joanna Cherry: I am focusing on internet connection records. There may be other questions about communications data, but I want to clarify, because it may be very important to Members' consideration of the Bill, that I am correct in saying that, if this Bill is passed as presently drafted, the assurance of anonymity on websites such as Crimestoppers will no longer be accurate because the purpose of internet connection records is to identify that A has used a particular device to connect to the internet service concerned.

Richard Berry: That is no different from the present situation with internet communications data. The fact that there is a freephone call number for Crimestoppers doesn't mean that in technical terms that communication cannot be traced, but we just don't do that because we guarantee anonymity. It wouldn't be necessary and it wouldn't be proportionate.

Q163 Joanna Cherry: But when you use a phone to contact Crimestoppers, there is no tick box saying, "I want to be anonymous", is there?

Richard Berry: There is an assumption. It is well advertised that Crimestoppers—

Q164 Joanna Cherry: There is no tick box on a phone.

Richard Berry: Not that I am aware of. No.

Q165 Joanna Cherry: But there is a tick box on the internet site saying, "I wish to remain anonymous."

Richard Berry: That can remain.

Joanna Cherry: That is there because we have discovered in police and law enforcement services, where I used to work as a Crown prosecutor, that if you guarantee people anonymity, you sometimes get more people to come forward.

Richard Berry: Absolutely.

Joanna Cherry: So it is possible that, if this Bill is passed, we will actually dissuade people from reporting crime because we can no longer guarantee their anonymity.

Chris Farrimond: I am also responsible for covert human intelligence sources for informants. Of course, we know their identity, but we guarantee their anonymity. That is precisely what we do, although their identity is known within the agency. It is difficult to predict exactly how this could possibly impact, but if we are guaranteeing anonymity, that means we will not—

Q166 Joanna Cherry: But we are not talking about CHIS; we are talking about ordinary members of the public, the sort of person who watches "Crimewatch UK" when it is on once a month, recognises one of the mug shots and goes on the website but is scared for their own safety and so wishes to remain anonymous. We need to be clear that that anonymity can no longer be guaranteed because all internet connection records will be collected. Is not that right?

Richard Berry: It would be guaranteed by law enforcement, because that is our operational policy. We would not access it. We do not retain the data, and nor could we access it, as a matter of policy.

Joanna Cherry: But the fact is that the connection to a particular service from a particular computer will be recorded as an internet connection record and retained.

Richard Berry: In theory, that could be the case, but it would never be accessed. Lots of internet connection records would potentially be gathered, but we are very much about targeted inquiry, rather than bulk inquiry, so it would never pass the necessity and proportionality test.

Joanna Cherry: That is an internal guarantee that you are giving us. There is nothing in the Bill to say that it would not be accessed, is there?

Richard Berry: Not that I have seen, no.

Q167 Mr Hayes: I will be mercifully brief. Given your very wide case experience, and the fact that an overwhelming number of serious crimes are now connected with both the technology and methods of modern media, can you envisage circumstances in which loss of life or severe injury might be prevented through equipment interference?

Chris Farrimond: Absolutely, yes.

Q168 Mr Hayes: That is something the Joint Committee recommended and now forms part of the Bill. On internet connection records, can you give us a flavour, also from your case experience, of the kinds of crimes and circumstances in which they might be vital to an investigation and, ultimately, to catching and convicting people involved in serious crime?

Chris Farrimond: Let us just start with the fact that internet connection records are the new comms data; they are the modern equivalent of comms data, the normal itemised billing that we have had for years and years. Criminals are using internet communications even if they do not necessarily realise it—when they send an iMessage, for instance, in an internet communication, rather than a text message. That is happening the whole time, and it is happening right across the population, whether people are law-abiding or criminal, so internet connection records now feature in every type of criminality. They are featuring more in those types of crime where the internet plays a larger part—fraud, for instance. I can talk about child sexual exploitation, where the internet makes it so much easier to share images, so internet connection records would be extremely useful for us in those circumstances.

Simon Grunwell: HMRC's business model going forward is to put more and more services online to enable taxpayers to do more themselves, a bit like an online bank account. We already have online frauds. We are quite attractive for fraudsters, in the sense that we collect £500 billion a year and we pay out £40 billion in benefits and credits. Comms data helps us directly prevent the loss of £2 billion in revenue. On the ICR point, in particular, we have already had online attacks against us. In one case alone we were able to prevent the loss of £100 million. ICRs can only help us in that regard.

Richard Berry: From a local policing point of view, it is not just about serious crime; it is also about—if I can use this phrase—policing the digital high street. So ICRs could be just as relevant for cases such as domestic abuse, stalking and harassment, to prove a particular case, or to help us deal with what might seem, in isolation, to be a minor issue, but can often be on a path of escalation to homicide or very serious assault.

Q169 The Solicitor General: You were just asked about anonymity and the perceived danger to anonymity—for example, in the Crimestoppers scenario—but that would apply if I telephoned Crimestoppers now, wouldn't it?

Chris Farrimond: It would.

Q170 The Solicitor General: Theoretically, you would be able to get access to the phone number that I have used and work out who that number was linked to and, presumably, link that to me now.

Chris Farrimond: Yes.

Q171 The Solicitor General: As I understand it, these internet connection records will be held by CSPs—communications service providers—not by the authorities.

Chris Farrimond: Correct.

Q172 The Solicitor General: In order to access those records, you have to apply to a SPOC, or via that procedure, and then a filtering process will apply.

Chris Farrimond: Yes, it does.

Q173 The Solicitor General: So the scenario of the authorities holding this information and being able, at a whim, to breach anonymity is nonsense, isn't it?

Richard Berry: We certainly very much follow the procedure of looking at each application and testing it for its necessity against its purpose, the proportionality, the levels of collateral intrusion and things like the timescales involved. If you look at the annual reports of the Interception of Communications Commissioner's Office in 2015, you will see that they even go to the extent—I think it was done on about 100,000 applications—of looking at the amount of time a decision maker, a designated person or, under the new legislation, a designated senior officer, actually takes to consider all the tests that are required to ensure that the parameters are tight and that justification is in place.

Byron Davies (Gower) (Con): In my experience, the UK is regarded as a world leader in intelligence-led law enforcement and I am sure that you agree that the Bill will enhance your capability. Can you tell me how important to your work it is that this legislation applies extraterritorially?

Chris Farrimond: It is rare for serious crime to be investigated and to have no international aspect to it at all. Certainly in the case of the National Crime Agency, almost every single case that we investigate has got an international aspect to it, but I suspect that that is the same for both my colleagues as well. That means that communications data will almost certainly be held in a third country at some point, because we have been communicating with people in other countries. The extraterritoriality will at least give us the ability to ask for those data. I do not doubt that there will be some complications when it gets compared with the host nation legislation along the way, but, nevertheless, at the moment we have a very lengthy process to get material back from other countries, so if this can help in any way, shape or form in speeding that up, that will be a good thing.

Richard Berry: It certainly is a strategic priority for law-enforcement policing to look at how we can ensure, as Chris said, this fragmentation of data across server farms, in clouds and across several countries is increasingly a challenge for us, so any legislation that can help with that process will be particularly useful.

The other point that I would make, building on what you said in your introduction, is also quoted by the commissioner in the 2015 report. Communications service providers, certainly in the US, very much favour the British SPOC system, because there is a dedicated, rigorous system, whereas they could perhaps be approached individually by—I think, to quote them—one of "10,000 FBI agents", all adopting a slightly different process. So we have got the right systems in place; I think it is really the relationships and the access that is critically important.

Simon Grunwell: I will just add that the internet obviously provides mobility and anonymity. We could have an attack from anywhere in the world, online, so we need to keep pace effectively with digital changes. Sometimes the only clue that we have as to who is criminally attacking us is a digital one. The ability to go extraterritorial to pursue that one clue could be vital.

Q174 Victoria Atkins: In the Government's response to the pre-legislative scrutiny, they refer to a sample of 6,025 referrals to the Child Exploitation and Online Protection Centre—CEOP—with which, I imagine, Mr Farrimond, you are very familiar. It says that of those more than 6,000 referrals, 862 could not be progressed and would require the ICR provisions in the Bill to have any prospect of being progressed. In other words, for at least 862 paedophiles out of that sample, you can go no further because you do not have the tools. Does that accord with your day-to-day working knowledge of this field?

Chris Farrimond: Yes, we get around 1,500 referrals per month, some 14% of which we cannot resolve. We cannot take them any further. Whether it is that number of paedophiles, or whether it is a smaller number who are sharing the same images, we cannot be sure, but the bottom line—the important thing—is that we cannot protect the child because we cannot resolve the data.

Q175 Victoria Atkins: Focusing on the point you have just made about protecting the child, a witness this morning referred to the collection of nude images and the security services apparently running facial recognition techniques on those images. Are such methods used to try to identify child victims so that law enforcement can find them?

Chris Farrimond: Yes, of course.

Q176 Victoria Atkins: Finally, on the extraterritoriality point, Europol is the EU's information and intelligence-sharing agency in The Hague. What sort of data do law enforcement across Europe share, through Europol, to try to tackle serious organised crime and for counter-terrorism?

Chris Farrimond: Quite a lot, actually. We feed into the Europol databases. We also, in fairness, have bilateral relationships, particularly when it comes to specific investigations, but for criminal data on themes, trends and so on, we will feed it into Europol to see if there are any cross-matches with any other country experiencing the same criminality.

Q177 Victoria Atkins: So in those two areas—counter-terrorism and serious organised crime—this legislation could help not just our country, but our neighbours overseas as well.

Richard Berry: Yes, absolutely. From experience, I was involved in running a national operation on human trafficking, and we basically created a dataset from a significant amount of intelligence gained during that national operation over six months. It went straight into the analytical work files within Europol and we were able to map organised criminality right the way back to mainland China in some cases. The added value point, which is what you are making, very much comes from that sharing.

Simon Grunwell: Can I just add to that? A significant thread for us is organised tobacco smuggling, which is international by default. So it can only help.

Q178 Gavin Newlands: Just a follow-up to a question asked in the last panel about ICRs as they relate to mobile devices and third-party apps. You brought up easyJet earlier, and I have got an easyJet app on my phone. As far as I am aware, it creates a lot of ICRs as defined in the Bill. There is no way to differentiate between an ICR that is created manually or automatically by a third-party app. How would that limit the operational effectiveness of ICRs for you?

Chris Farrimond: To go back to my previous answer on this point, from your mobile record—the ICR from that—we would require your provider, Vodafone or whoever, to help us to understand which flight provider you were using. If they came back to us and said, "One of the domain names is easyJet", we would say, "Thank you very much." That is what we would expect from Vodafone. We would then go to easyJet and say—with the right authority signed off, obviously, and with the proportionality, necessity and everything that goes with that—"Can you tell us about his travel plans?" They would, hopefully, be able to do precisely that with the data that they hold on their flight details. But as for the actual app, all that we would look for from your provider would be to tell us that you have been making use of easyJet, and that would give us the next point in our investigation.

Gavin Newlands: I might not have used easyJet for several months, but the app still connects my phone to easyJet's service provider. Likewise, I have a British Airways app. None of that limits any effectiveness for you?

Chris Farrimond: What I would expect to get is something showing you connected to easyJet for two minutes rather than for a nanosecond, or for an upgrade coming through. If we saw two minutes, we would say, "He did something with easyJet at that point."

Richard Berry: Things like the tracking cookies you have on normal websites are not relevant information for our purposes. To offer a point of reassurance, we have a decade of experience of looking at what relevant data should be retained. ICRs are no different to that principle. Prior to any retention notice being served on a particular provider, law enforcement, the Home Office and the provider will be looking at the operational benefit, the cost and the technical feasibility of what data they hold and what data we would use. It almost takes each provider on a case-by-case basis to ensure we are gathering only relevant information. We could see those feeds back—the little connections you are talking about—being ruled out of the data we need to retain.

Q179 Keir Starmer: May I go back to the definition of internet connection record? To take it in stages, you are obviously concerned about your ability to deal with serious crime and the visibility of what you can do; I completely understand that. You make an ask of the Home Office, which as you said, is basically, "Who? When? Where? How?" That is where you think you need to go next, to maintain the ability you have now, because of the different ways people are communicating.

From that, you said, "Well, therefore *The Guardian* is enough for us, not that someone went to a page on Libya or clicked on something about Libya bombings, because that is not within our ask." My difficulty is not to challenge why you want that, what you use it for or its utility. I just cannot see how the definition in the Bill is limited to your ask; in other words, it appears to go as far as you want to go.

Tell me if this is an unfair question, because it is about the words on the page, but which bit of the definition you understand to be the word or words that limit it to what you say you are asking for, rather than letting it go any further? At the moment, I cannot see that bit of the jigsaw. In other words, which is the trigger word in the definition of internet connection record that says *The Guardian* website but not "within *The Guardian*, the words 'Libya' or 'bomb'" or whatever it may be that means we cannot go beyond what you have asked for?

Chris Farrimond: It is a bit difficult for us, because as law enforcement officials, we have no hand in writing the Bill.

Keir Starmer: Fair point.

Chris Farrimond: We simply have presented our case to the Home Office, and in quite some detail we have explained what we think we need to be able to protect the public. I am afraid I cannot speak to the actual words on the page.

Q180 Keir Starmer: Can I follow that question with this last one? If the definition were to be reworded in a way that reflected what you had asked for but made absolutely clear that it did not go beyond that, would that not trouble you at all? In other words, if there were a word, a phrase, a group of words or a definition that made it clear in technical, legal terms that we are talking about *The Guardian* but not certain clicks within *The Guardian* website.

Chris Farrimond: As long as it meets the requirement we have put forward, absolutely.

The Chair: Joanna Cherry, you have five seconds, and anyone who wants to answer has 10 seconds.

Q181 Joanna Cherry: I will try. Unilateral assertions of extraterritoriality will not help us much, will they? What we need is bilateral or multinational agreements with other countries, such as we have through Europol.

Chris Farrimond: I would say that they will help, in that they demonstrate what the UK would like to achieve. We have really good partnership relationships with a number of countries around the world. If it so happens that they are looking at a similar sort of provision in their legislation, we could quite easily find common ground. It may be that that is not possible and we need greater detail, but there is no harm at all in saying, "Look, this is what we're asking for. It's quite reasonable, isn't it? These are our checks and balances around it." That is the start point, as far as I can see, for further negotiation.

The Chair: Thank you. Well done colleagues—you were razor-like in your questioning.

Examination of Witnesses

Mark Astley gave evidence.

3.30 pm

Q182 The Chair: We are down to one witness. Mr Astley, would you introduce yourself very briefly?

Mark Astley: I am the head of NAFN Data and Intelligence Services.

The Chair: Fantastic—that is an even shorter introduction than the one I have in front of me that details your distinctions.

Q183 Keir Starmer: From your perspective—the anti-fraud perspective—which of the powers in the Bill are most important to you and why?

Mark Astley: The powers to access communications are very important to our members. Trading standards are our main users. They are not high users but it is important for them to be able to investigate those crimes so they can support their community and the businesses that they are working for and on behalf of.

Q184 Keir Starmer: At the moment, you do not have access to internet connection records.

Mark Astley: Correct.

Q185 Keir Starmer: How does that inhibit you, if at all?

Mark Astley: At present, the impact is uncertain.

Q186 Keir Starmer: The impact of not having it.

Mark Astley: Of not having it—yes. There are areas, as colleagues have previously mentioned where, in the digitisation world that we are moving towards, everything is being conducted over the internet. That is something that may affect and have an impact on investigations for local authorities.

Q187 Keir Starmer: But at the moment you cannot say how not having it affects your ability?

Mark Astley: No.

Q188 Keir Starmer: And what do you think you will get when you get access to internet connection records?

Mark Astley: At the moment, I understand that we are not going to receive that access. Local authorities are not being included in having access to internet connection records.

Q189 Keir Starmer: No, local authorities are not.

Mark Astley: No, but some of the other public bodies may get access to that. That would give them the front door to the internet provider that they have entered.

Q190 Keir Starmer: But your network is not just limited to local authorities.

Mark Astley: Currently it is for communications data, as the legislation stands.

Q191 Keir Starmer: Within your network, what are the other bodies and agencies?

Mark Astley: Can I just elaborate a little bit more about our organisation? We provide a service to assist them in obtaining data and intelligence to assist investigations. However, from a telecommunications perspective, we are only able legally to operate on behalf of other local authorities. We are not able to represent other public agencies such as the Food Standards Agency, although the intention of the Bill is to introduce those collaboration agreements, so we could facilitate that.

Q192 Keir Starmer: I see, so at the moment, your function is limited in this particular field to local authorities.

Mark Astley: Correct.

Q193 Joanna Cherry: Your organisation has identified a range of crimes that local authorities use communications data to tackle. Do you think the Bill ought to identify the crimes more precisely to prevent data from being used in relation to, for example, rubbish collection or school places?

Mark Astley: I believe that the process is in place for identifying necessity and proportionality. The three bar process that we currently have in place will deal with that. To actually identify particular legislation could become more constraining and difficult to administer and, as more legislation comes along, more changes may be required to the Bill.

Q194 Joanna Cherry: Do you agree that the issues of rubbish collection or potential abuse of school places are not really serious crimes?

Mark Astley: I do, and the fact that communications data is not used for those types of investigations in respect of that should enforce that.

Q195 Joanna Cherry: But there is nothing on the face of the Bill to prevent it from being used for that kind of investigation, is there?

Mark Astley: No, but we have the three locks in place. They call it the double lock at present, but what the National Anti-Fraud Network provides is what we call a triple lock. We have the NAFN single points of contact that it has to go through. They are fully accredited and professional, and they are fully trained to ensure that we weed out all those types of inquiries. The next lock is the designated person, and following that you have the judicial approval process, too. There is a triple lock in place to prevent any of that from happening.

Q196 Joanna Cherry: But there is nothing on the face of the Bill to prevent the individuals you have mentioned from ultimately reaching the view that it might be necessary or proportionate to access communications data to deal with issues around rubbish collection or school places. It has happened, has it not?

Mark Astley: Not for communications data. The process is in place—the triple lock—from a NAFN perspective. The NAFN SPOCs are totally independent and fully trained. They will ensure that any application is appropriate, necessary, proportionate and lawful for that to process.

Q197 Joanna Cherry: You mentioned judicial authorisation. Can you elaborate on what you meant by that?

Mark Astley: Currently, our members have to go to a local magistrate to have any access request approved judicially.

Q198 Joanna Cherry: It is possible to bypass the single point of contact in an emergency, is it not?

Mark Astley: No, not for a local authority.

Q199 Joanna Cherry: Your organisation told the Joint Committee that five hours of an officer's time seeking judicial approval is "slow and inefficient" and "a deterrent to councils". Do you feel that the individual's right to privacy might justify five hours of an official's time?

Mark Astley: The issue around resources is more about how we can better deliver the services. The judicial approval process is there, and it is supportive. Looking at the figures for the past two years, 2% of those requests have been rejected by our own SPOCs, 0.3% have been rejected by the designated persons and only 0.2% have been rejected by judicial approval. Our belief is that the processes in place work effectively.

Q200 Joanna Cherry: That was not really my question. My question was on whether you agree that the individual's right to privacy justifies the time that is sometimes taken in inputting for a judicial approval.

Mark Astley: I understand the need for respect for privacy, but the necessity and proportionality aspect of every case will be considered, and if it is appropriate to do so, we would need to intrude on that privacy.

Q201 Mr Hayes: Obviously, your role is an additional safeguard. There are those who think that the Home Secretary and I are preoccupied with safeguards, checks and balances and the defence of privacy, but I think we have probably got this right. Can you tell me of the number—the frequency—of requests that you would consider to be an abuse of power in respect of applications for information? How often do you come across seedy requests that you would consider to be an abuse of the powers?

Mark Astley: In 2% of inquiries in the past two years, we have had applications rejected or cancelled through the input of our accredited SPOCs.

Q202 Mr Hayes: Is that common?

Mark Astley: It is actually going down because of the training and the accreditation that is provided by our staff—the figure has reduced every year—so that people are fully aware, fully trained and fully focused on what is appropriate, what is necessary and what is lawful.

Q203 Mr Hayes: But most requests are reasonable, sensible and measured.

Mark Astley: They are.

The Chair: Have you finished, Mr Hayes?

Mr Hayes: I have finished, yes. You asked me to be brief.

The Chair: Actually, on this occasion I did not ask you to be brief, but thank you for being brief in the spirit that that was offered.

Q204 Victoria Atkins: Just so there is no mystery—people might ask themselves, "Crikey! What on earth do local authorities need these powers for?"—what sort of offences do local authorities investigate and prosecute?

Mark Astley: Local authorities have been provided with a wide remit in legislation to assist them in investigating a wide range of high crimes and serious crimes, which can range from rogue traders to dangerous goods and fake alcohol and tobacco.

Q205 Victoria Atkins: In some cases, fake alcohol can be fatal.

Mark Astley: It can be fatal, yes. There was a recent case of children's clothing that was not fire retardant. It is important for those officers to react quickly to prevent any loss of life or serious danger to life.

Q206 Victoria Atkins: They also prosecute housing benefit fraud, don't they?

Mark Astley: Not any more.

Q207 Victoria Atkins: Do they still prosecute landlord offences?

Mark Astley: Yes. Tenancy fraud offences as well. There is also internal fraud. There was one specific case where people were setting up rent accounts and filtering thousands of pounds from within the organisation.

Q208 Victoria Atkins: But, just as importantly, and probably more importantly, they can also safeguard the lives of people who are renting properties from landlords who, for example, are not keeping up to date with their gas certificates.

Mark Astley: That is correct.

Q209 Victoria Atkins: Just to be clear, under this Bill local authorities will not be entitled to internet connection records.

Mark Astley: That is correct.

Q210 Victoria Atkins: I do not know whether you have already done this, but could you briefly help us with the process that exists at the moment? What will happen after the Bill in terms of your organisation getting this information?

Mark Astley: In how we deal with an inquiry?

Victoria Atkins: Yes.

Mark Astley: Inquiries come through to our organisation electronically from an applicant, and our SPOC will work with the applicant to get the application either up to standard or cancelled because it is not appropriate. Once it is up to the required standard, the application is passed over to the designated person, who will then look to authorise it for proportionality. Once that has gone through, our systems provide a court pack, which is delivered to each individual applicant, and they then have to arrange for a court attendance to get judicial approval.

Differently, in Scotland they also have a legal representative process, except they have a fourth lock in place in that their legal representatives get involved and then go on to the sheriffs for judicial approval. It is then returned to us. Once we have that approval, we then obtain the information accordingly.

Q211 Victoria Atkins: Of course, the Bill also introduces the further safeguard of the criminal offence of making an unauthorised disclosure. In other words, there is also safety from the perspective of the telecommunications organisation, BT or whoever it is, knowing that if they do not make sure that you have complied with all of your duties, they themselves may be criminally responsible for giving you any information that they should not be giving you.

Mark Astley: Yes, and I think there is an intention to make the SPOC—the single point of contact—responsible for any recklessness or wilfulness in that misuse. That is another safeguard in place to ensure that there is no abuse or misuse of telecommunications data.

The Chair: With the permission of the Committee, I might suspend the sitting for 10 minutes at 10 minutes to 4 to allow people to have a quick break, because this is quite a long sitting. Is that with the permission of the Committee? Brilliant.

Q212 Christian Matheson: I have two questions. Mr Astley, there are two opposing schools of thought relating to this Bill. There are those of us who recognise the need to update the legislation as it is to provide protection for children against sexual abuse and to provide protection against terrorism, terrorist atrocities and terrorist threats, and at the far end of the scale are those who believe that there is an absolute right to privacy and that no price is worth paying to imperil that privacy.

The job of Parliament is to find the correct balance on the scale between those two extremes. I do not think it would be too difficult to find justification, for example, for the protection of children against sexual abuse or for the defence of the realm against foreign threats and foreign terrorists. Justify to the Committee, if you will, the use of some of these powers, limited though they are in the Bill, for offences at the lower end of the scale.

Mark Astley: From a local authority perspective, they are a small user of telecommunications data. It has never been abused or misused from a local authority perspective, but they investigate some quite serious crimes. We had a particular case of advance-fee fraud, which was worth £7.5 million.

If you look at the majority of the applications that local authorities make, an extremely high percentage in the last two years—96%—was purely for subscriber data, or what is currently known as "c data". That is the basic information about the subscriber to a telecommunication service and sometimes that is the key information that investigators need. An example would be someone who is trafficking illegal tobacco and the shopkeepers they are speaking with only have a telephone number for the delivery person. Therefore, in order for people to investigate successfully, which they have the powers to do—provided by Parliament—it is important that they have that access.

Q213 Christian Matheson: Let me ask you then, finally, why in that case, if a crime is sufficiently serious, can the involvement of the police not take over the requirements for access to electronic communications data, as opposed to, for example, your members?

Mark Astley: Yes. As I have previously mentioned, our members are very highly trained; they are commensurate in some respects to what the police investigate. But they deal with their local community on a more local basis and they have the powers and expert knowledge, in particular about rogue traders, about illicit tobacco and about counterfeit items. They have that experience.

Q214 Christian Matheson: You could still handle those investigations and deal with them, but when it was apparent that they are of a sufficiently serious nature you can involve the police, who are then able to make the applications on your behalf, so you would not need access under the terms of the Bill.

Mark Astley: It is a valid point, but I believe that the powers are there for the trading standards, who do a really good job, and they have done an excellent job so far in dealing with high-level crime.

Q215 The Solicitor General: In the last year for which records are available, which I think is 2015, about half a million applications for access to comms data were made. About 0.4% of those were local authority applications.

Mark Astley: That is correct.

Q216 The Solicitor General: So we are talking about several thousand out of about half a million. Is that right?

Mark Astley: Well, if you look at the last two years alone, we are talking 3,300.

Q217 The Solicitor General: You were asked questions about the replication of the existing regime relating in England and Wales to magistrate authorisation, in Scotland to sheriff authorisation, and in Northern Ireland to district judge or magistrates court authorisation, for applications for access to comms data by local authorities. Those provisions are replicated in the Bill, are they not? I think it is in clause 66. But they are in the primary legislation.

Mark Astley: They are.

The Chair: Colleagues, I think we could do with a 12-minute break, because people have to get coffees and check with their offices.

Sitting suspended.

Examination of Witnesses

Lord Judge, Clare Ringshaw-Dowle, Sir Stanley Burnton and Jo Cavan gave evidence.

4 pm

The Chair: Welcome to the panel. In a matter of a few words, please introduce yourselves.

Jo Cavan: I am Joanna Cavan. I am the head of the Interception Commissioner's Office.

Sir Stanley Burnton: I am Stanley Burnton. I am the interception of communications commissioner.

Lord Judge: I am Igor Judge, the chief surveillance commissioner.

Clare Ringshaw-Dowle: I am Clare Ringshaw-Dowle, chief surveillance inspector.

Q218 Keir Starmer: Thank you to our distinguished panel for their time this afternoon. I think this is a first—me asking distinguished judges a question. It has always been the other way round for my entire career. I shall try to keep it short and sweet.

Can I start on the issue of the approval of warrants by judicial commissioners under the Bill, and the proposed test? Clearly judges perform different functions every day. One function is to issue a warrant—to search a premises, for example; judges do that day in, day out. They are the decision maker. An application is made to them and they look at it and make their own decision, and they issue or do not issue the warrant as the case may be.

A different function is a reviewing function—a public law function where a judge is essentially reviewing somebody else's decision. On my reading of the clause on approving warrants, clause 21(1) and (2)—if you do not have it in front of you, I have copies of it—it appears to be clearly a reviewing function. The judge is reviewing the decision of the Secretary of State, not actually making a decision him or herself on the warrant. Do you agree with that?

Sir Stanley Burnton: I do, certainly.

Lord Judge: I agree too, but you have a problem: what do you mean by judicial review?

Keir Starmer: Can I explore that?

Lord Judge: You asked me for a short answer, and that is a short answer. *[Laughter.]*

Q219 Keir Starmer: Judicial review covers a range of different approaches depending on subject matter, intensity of review and so on. As worded, how much deference or margin do you anticipate judges will give to the decision maker, the Secretary of State, in exercising these functions?

Sir Stanley Burnton: In theory, you have a complete spectrum. A judge can operate at one end of the spectrum when he just accepts what the authority is putting to him, and at the other end he can be quite stringent in reassuring himself that the statutory tests have been properly applied and satisfied. Frankly, it is going to be the commissioner who will decide—fairly early on, I would have thought—how stringent the test should be in this case. My own view is that it should be quite stringent, approaching the one that was applied in the case of control orders.

Q220 Keir Starmer: Do you agree with me that as the Bill is currently drafted, it is not clear what Parliament intends, and therefore it will fall to the judges? In other words, it is broadly enough drafted to cover a longer-arm review or a closer intense review depending on what judges decide as cases evolve. It could accommodate both approaches.

Sir Stanley Burnton: It is left to the judges, is it not, to decide what the proper approach is?

Keir Starmer: On this draft.

Sir Stanley Burnton: On this draft. It may be difficult to draft more tightly. The other thing I would say is that whether the judge is a decision maker or an approver, he necessarily has to give a lot of weight to the opinion of the person who is making the application to him.

If the secret service is saying, "Our assessment of this man is that he is a dangerous terrorist", it may be very difficult to go behind that, and there is no reason why the judge should go behind it unless there is material before him that indicates that that is a wholly unreasonable and unsupported assessment. But you are compelled to give weight to the opinion of the people who are actually involved in whatever the subject matter is.

Lord Judge: I do not go all the way along the route with Sir Stanley about this. I think "judicial review" is a very easy phrase to use. It sounds convincing, but it means different things to different people. People say, "Wednesbury unreasonableness"—that was a case decided by the Court of Appeal in 1948 or 1947, and it has evolved. Personally, I think that when Parliament is creating structures such as these, it should define what it means by "judicial review". What test will be applied by the judicial—I call him that—commissioner, so that he knows what his function is, the Secretary of State knows what the areas of responsibility are and the public know exactly who decides what and in what circumstances? I myself do not think that judicial review is a sufficient indication of those matters.

Q221 Keir Starmer: Thank you. Sticking with functions, if I may, as the Bill is drafted, the body responsible for authorising investigatory powers, as we have just described, is also the body responsible for oversight after the event. On the face of the Bill, there is no structural distinction between those functions. Is that sensible, or could it be improved?

Lord Judge: As that is the way in which the surveillance commission works, I strongly recommend it to you. There are different people exercising different functions. The pre-authorisation that goes on in our section of the system involves a commissioner being satisfied—I am sure you all know about the relevant tests—and either agreeing or not agreeing; that is a very important moment. In most cases, happily, because people make responsible applications, they are agreed to. Sometimes it is suggested that they should be amended, and very occasionally they are refused.

That process then unfolds, and whatever happens happens. My inspectors annually inspect the entire force—not just the individual who made the application in the first place, but each police force and each prosecuting authority—to see whether their systems are effective and check, and not just on the ones that have come through, to ensure that the process was brought to an end speedily or, when nothing further happened, that the authorities did not go on too long and so on. It is also to ensure that when the authorisation was originally given, it was founded on proper evidence and then correctly given.

Normally, this has all worked perfectly well, but there is a danger in underestimating the value of the inspectors; I shall come to a different point on that when I can give a longer answer. The process works very well in this way. They report to me as chief surveillance commissioner. I then digest the report and go see the chief constable of each force, or get one of my commissioners to go see them, to say, "This is where you are going wrong, and this is where you must do this and that."

That is because the inspectors have taken the thing apart. They go to police forces for days; the whole lot of them go to the Metropolitan police for a week. They have

[Keir Starmer]

the right to see anything they like, and they demand to see it. The commissioners would not be best able to exercise that function, because they are judges. They are not qualified.

Jo Cavan: There are a number of important points around these clauses in the Bill. First, we are really disappointed to see that although the Government are talking about creating a world-leading oversight body, the clauses as currently drafted do not actually create a commission. They simply create an investigatory powers commissioner and a number of judicial commissioners.

When we look at approval by those commissioners, the reality is that they are only going to be approving 2% of the authorisations that will actually be undertaken under the Act—arguably, the more highly intrusive authorisations. The remaining 98% of authorisations will only be overseen post facto, and the reality is that they will be overseen by staff within the commission.

If we look at some of the judgments coming out of the European Court of Human Rights and the European Court of Justice, there are some really important safeguards on post facto oversight, looking at the retention, storage and destruction of material, how it has been used and any infringements or breaches around the acquisition post-approval. We really feel that the Government need to create this body in the clauses.

Q222 Keir Starmer: One final swift question on thematic warrants and the breadth of the powers proposed in the Bill. Do any of the witnesses have headline concerns that the Committee can take away to work on as we consider the Bill line by line?

Sir Stanley Burnton: First, the existing formulation in RIPA is very unsatisfactory and unclear, and it does not cover many cases in which it would be sensible to have a so-called thematic warrant. However, the wording of clause 15(2) is very wide. If you just have a warrant that gives a name to a group of persons, you have not identified—certainly not in the warrant—all those persons to whom it is going to apply. There could be substantial changes in the application of the warrant without any modification. At the moment, the code of conduct envisages a requirement that names will be given so far as practicable. Our view is that the warrant should name or otherwise identify all those persons to whom the warrant will apply, as known to the applicant at that date.

The other concern is that substantial modifications can be made to a warrant under the Bill with no judicial approval or even notification. That needs to be changed.

Lord Judge: I agree with Sir Stanley. I will not say anything more on the second point he made, but on the first, a part of the process that all of us involved in supervising surveillance attach a great deal of weight to is that we are looking at individuals. There has to be evidence that X requires this, that there is a situation in which it is necessary for this to happen, that it is proportionate in this particular individual's case and that there is no collateral interference. For example—there are many different examples—why should a women who happens to be married to or living with a man who is suspected and so on have her life entirely opened up in this way? Not having specific identified individuals leaves a very delicate situation. I suspect that the commissioners would find it very difficult to just say, "Well, we're satisfied. There's this gang here and they're all pretty dangerous." They might not be, and we have to be very alert to that.

Q223 Joanna Cherry: I have questions for Jo Cavan. In your organisation's written evidence, you have picked up on earlier concerns about the draft Bill and updated them in the light of the finalised Bill. In the first point, you say that you have concerns about the "aggressive timeline" for the Bill. Can you explain what you mean by that?

Jo Cavan: It is a really complicated and significant piece of legislation. Although I broadly support the Bill, because it is a good thing to put a number of the powers used by the intelligence agencies on a clearer statutory footing and to try to improve transparency, I do think that the scrutiny process has been very hurried. That is of concern because there are some significant privacy implications to the clauses in the Bill. There is still a long way to go towards strengthening some of the safeguards. Also, a lot of the operational detail is in the codes of practice. It is really important that those are scrutinised properly, line by line.

Q224 Joanna Cherry: When you express concerns about the aggressive timeline for the Bill, are you talking about the Bill before us as well as the draft Bill?

Jo Cavan: Yes.

Q225 Joanna Cherry: So you consider the time that has been afforded for the scrutiny of the Bill before us to be aggressive.

Jo Cavan: It has been challenging to say the least.

Q226 Joanna Cherry: Do you think it is adequate?

Jo Cavan: You could argue that because we are waiting for a number of key judgments from either the European Court of Human Rights or the European Court of Justice, it might seem a bit premature to be legislating in some of these areas, but then when do you draw the line?

Q227 Joanna Cherry: At point 5 in your written evidence, you pose the question:

> "Is it desirable to have the same body responsible for authorising investigatory powers and undertaking the post facto oversight of the exercise of those powers?"

You say:

> "If so, the judicial authorisation and oversight elements of that body must be operationally distinct."

You have already explored point 2 of your written evidence with us, but will you elaborate on point 5?

Jo Cavan: It is clear to us that there needs to be some operational distinction between the approval—the judges who are going to be approving some of these techniques—and the audit and oversight after the event, because if the judges approving the requests are then responsible for the post facto oversight, essentially they could be accused of marking their own homework. Again, if the commission is created, you will be able to distinguish those key elements.

It is really important for the commissioners to work very closely with the inspectors and technical engineers and so on who will carry out the post facto audits. They are obviously going to need to support each other, but it is really important that there is a distinction. I think I have spoken to a number of our international oversight counterparts, and some of those are quite surprised that we are going down a route where we are putting both elements into one body.

Q228 Joanna Cherry: At point 6 of your written evidence you expressed concern that in the draft Bill there were

"a number of clauses which provide exceptions for national security or which exempt the intelligence agencies from key safeguards".

What is your view of the finalised Bill in relation to that concern?

Jo Cavan: Essentially there has been progress on one of the national security exemptions, which is around the acquisition of communications data to determine journalistic sources. The Government have amended clause 68 to remove the national security intelligence agency exemption. That was because that was picked up by the Intelligence and Security Committee and the Joint Committee.

However, there are still two broad exceptions in the Bill: clauses 54 and 67. One of them is really important, because it is around the independence of designated persons. This area was strengthened as a result of the Digital Rights Ireland case, and that is an area where we still find significant compliance issues within public authorities. Communications data is approved by designated persons—it will become designated senior officers in the Bill—who are from the same public authority. In almost half of the police forces, intelligence agencies and other bodies that we inspected last year, we made recommendations around that area because we were not satisfied with the independence.

The clauses as drafted seem to drive a horse and cart through the independence requirements for designated persons by exempting very broadly national security. The same is the case in the single point of contact provision in clause 67: that appears to exempt in national security cases the SPOC being consulted, and we see the SPOC as a key safeguard in the process. So the fact that the Government have already said that the exemption relating to journalistic sources was broad, and removed it, suggests that the same needs to happen to clauses 54 and 67.

Sir Stanley Burnton: I would just like to add that it is far from obvious that the interests of national security, which is a ground for the grant of a warrant, is itself an exceptional circumstance. It is very difficult to see what the logic behind that formulation is.

Q229 Mr Hayes: Joanna, I guess you are pretty familiar with the legislative process and the way Parliament works.

Jo Cavan: I would hope so.

Q230 Mr Hayes: Good. How often have you encountered a Bill that before its publication in draft had been preceded by three reports, and which was subsequently considered by three Committees of the House before embarking on the normal process of scrutiny? Can you think of another Bill in the last 10 years like that? How many can you list?

Jo Cavan: I am afraid I cannot think of any off the top of my head, but I will say the reviews—

Q231 Mr Hayes: You said it had been hurried; that is what I was trying to get at.

Jo Cavan: Yes, absolutely. The reviews were comprehensive in their own right. However, the three reviews that you talk about were specifically focused on certain areas. David Anderson was specifically focused around interception and communications data, so he did not look at equipment interference, for example. Some of the capabilities had not been avowed at that stage, so they are seen for the first time in the Bill. I think it is a challenging timeline, and a number of the witnesses have talked about their concerns.

Q232 Mr Hayes: But I just wanted to establish, just to be clear, that in my 20 years I cannot think of a Bill that has had quite such extended scrutiny. I am sure there must be some, but they do not spring to my mind and they clearly do not spring to yours, either.

Jo Cavan: No, that is right.

Q233 Mr Hayes: On a second point of fact, you talked about the number of cases in which judicial approval is involved. That is the double lock. The double lock applies where a Minister—the Secretary of State for Northern Ireland, the Foreign Secretary or the Home Secretary—issues a warrant. The double lock applies where one of those people is involved. That is right, is it not?

Jo Cavan: That is right.

Q234 Mr Hayes: You would hardly expect the second part of the lock to apply where a Minister is not involved, would you?

Jo Cavan: The figures from last year that were published by all three commissioner bodies show that only about 7,000 out of 290,000 applications actually have judicial approval.

Q235 Mr Hayes: Where the Minister is involved. So the judicial approval is a double lock, and therefore the second part of the lock applies where the first part applies.

Jo Cavan: Not in all instances in the IP Bill, but in the majority, yes. There are still some exclusions.

Q236 Mr Hayes: On a separate point, it has been said that the judicial commissioner—this is a question for any of you, but I am thinking of the two gentlemen in the middle in particular—will not be sufficiently independent, and that they will be deferential towards the politicians involved. Is that your view? Are they likely to be deferential, or are they likely to act independently?

Lord Judge: I think you should ask the last 10 Secretaries of State whether they had an easy time when judges have had to consider whether they are acting lawfully. You will find, I suspect, that many of them feel fairly scarred by the experience. There is no danger whatever.

Q237 Mr Hayes: I have known a number of Home Secretaries, and none of them has suggested that the judiciary is deferential. I take your point. Finally, in terms of the appointment of the judicial commissioners, would the Judicial Appointments Commission be a better place to appoint them, or do you rather like the model we have come up with?

Lord Judge: No, I much prefer the model you have come up with. The Judicial Appointment Commission appoints judges usually from people who have not been judges. This is an appointment system that will work for people who have already been through the process, have acted as judges, have been appointed at whatever level they have eventually ended up, and are then exercising a new function. There is no point whatever in involving the Judicial Appointments Commission, ignoring the fact that it has got far too much to do anyway and not enough people to do the work.

My concern about the appointments is the speed with which all this is going to happen. We are going to have, under clause 233(3), a new investigatory powers commissioner within two months of the Bill becoming an Act. Where is this wonderful individual, male or female, going to come from within two months? The processes of appointments that I have had anything to do with take a very long time. I announced my retirement in November 2011 to be replaced by October 2013, and nobody knew who the next Lord Chief Justice was until the end of July. I am very worried about that. It is a very serious point. It is not a big point, but it is serious.

Mr Hayes: We must all rise to the challenge.

Q238 Peter Kyle: Sir Stanley, in response to Sir Keir's question, you said that you felt that judges would be compelled to give weight to the person applying. Will judges, considering that it has been signed off by the Home Secretary, feel compelled to give weight to the fact that the Home Secretary has already authorised the warrant?

Sir Stanley Burnton: Well, you give weight to it, but you none the less look at the material to see whether she was entitled to come to the decision she came to.

Q239 Peter Kyle: There is a lot of weight already by the time it gets to the judge to make the decision, so the bar is high for you to overturn the application.

Sir Stanley Burnton: These are serious matters. To authorise or to approve a warrant is a serious matter, but equally not to may be a serious matter.

Q240 Peter Kyle: Thank you so much for a great answer. Joanna, following on from the Minister's question, have you ever come across a Bill of this complexity, size and importance in your career?

Jo Cavan: No.

Q241 Peter Kyle: So it is unique, and therefore the conditions that lead up to it are unique as well.

Jo Cavan: That is right, although I defer to the individuals in this room who have been involved in this type of stuff for far longer than I have. Six codes of practice containing the operational detail were published on 1 March accompanying the Bill. That is a huge amount of material to examine.

Q242 The Solicitor General: May I go back to the first points made about the judicial review test? I put in a plea for the poor parliamentary draftsmen and women who work very hard indeed to try to strike a balance between avoiding excessive prescription and the dangers of being unduly vague. Lord Judge, you suggested we were falling more towards the latter end of the spectrum and being somewhat unhelpful.

There are in clause 18 the necessity criteria that are applied by the Secretary of State and then by the commissioner. The difficulty I have is, what do I do? I am trying to ensure the commissioners have discretion and the ability to make a nuanced decision based upon the individual case before them. At the same time, I am being told, "Well, that isn't good enough." Should the draftsmen produce a non-exhaustive checklist, or is that in itself full of dangers for the commissioners when it comes to their decision making?

Lord Judge: I think it is a matter of principle that has to be decided by Parliament—of which I am a Member, in the other place. What check is appropriate for Parliament to put on the Secretary of State exercising this very important power?

The Solicitor General: That is there; it is in clause 18.

Lord Judge: There it is. If you leave it as judicial review, we know that judicial review depends on the context, on when you have last been in the Supreme Court and when the last case came from the European Court of Human Rights; it is a flexible concept. That is one of its strengths, but I am not sure that in the context of the public responsibility that goes with the issue of these warrants there should be a flexible concept.

The Home Secretary has to make the decision. As it happens, if there is the equivalent of Brussels here in London, she will now be there. She will be answering. She will say, "I did issue this warrant," or "I didn't." Whichever way she did it, she will be responsible and answerable to you. What is the role of the judicial commissioner in such an arrangement? Does he come before you too, because he said, "I don't agree with this warrant," or, "I do agree; I do support it"? We need to be clear what you want the commissioner to do. Not everybody agrees with me, but I think that just saying "judicial review" is not clarifying where responsibility rests at the really crucial moment, which is when disaster strikes.

Q243 The Solicitor General: But you appreciate the problem that we have in getting this right.

Lord Judge: I do, but that is what Parliament is for. We have to decide what the law should be. I myself would like the law on this issue to be absolutely unequivocal, whatever Parliament or the House of Commons ultimately want.

Sir Stanley Burnton: We wonder what the function of clause 196(6) is. It is either telling a judge the obvious or it is a big stick to wave at the judge, to say, "You have to approve this because if you don't, you'll be jeopardising the success of an intelligence operation."

Q244 Suella Fernandes: Building on the point made by the Solicitor General, clause 21 sets out the "necessary" and "proportionate" tests. We have heard a lot about those words. What questions do you ask when you are assessing proportionality? What is that analysis?

Sir Stanley Burnton: You are looking at the effect of the measure in question as against alternatives and as against the mischief that is aimed at—are we talking about saving life, or it just a matter of money? If it is money, is it a lot of money? Is it pensioners' money or the Government's? You weigh one up against the other, and in the end, it is a matter of assessment—looking at one and looking at the other.

Q245 Suella Fernandes: So reading that meaning of proportionality, which we all agree on, with the factors listed in clause 18, is it not clear to a decision maker what factors are relevant and the level of scrutiny to be applied?

Sir Stanley Burnton: You have had my answer already. I am content with the Bill as is, but Lord Judge takes a different view.

Lord Judge: The answer surely is that those criteria are applied by the Secretary of State. The commissioner will apply the same criteria, but are you asking him or her to be a co-decision maker or a supervisor of the Minister? If a supervisor, then you have to define what his or her role should be.

The Chair: Thank you very much, panel. Have a happy Easter and enjoy your weekend reading.

Examination of Witnesses

Lord Reid and Charles Clarke gave evidence.

4.30 pm

The Chair: Thank you, both distinguished former Home Secretaries. I will not ask you to introduce yourselves because I think that would be a little impertinent of the Chair. Let us go straight to Keir Starmer.

Q246 Keir Starmer: Thank you both for coming to give evidence to us this afternoon. We are really appreciative. Can I dive in with the question that I think the whole Committee is intrigued by or interested in? You have experience of carrying out authorisations and signing warrants. We know there are a number every day. Can you give us an example of the exercise you both carried out when you were looking at warrants so that everyone in the Committee can understand what the role of the Secretary of State was before, as is now proposed, it goes off to a judge or commissioner?

Charles Clarke: The submission is made by the officials and the services, and says there is a suspected threat in a certain area and that they recommend authorising a power to surveille a group of individuals. The judgment that the Secretary of State then has to make is whether he or she does or does not accept that there is a case for surveilling the individual. According to the time available—some of the issues do not give you a great deal of time to decide what is happening because things can be moving very quickly in both serious and organised crime and counter-terrorism—you might decide to seek more information about the particular circumstances and why the judgment is being made. I think that you would always—I don't know what John's experience was—have at least a brief discussion with the officials concerned about the particulars of the case. It would not necessarily be extensive and the longer you are Home Secretary, the more experience you gain of the circumstances in which these sort of things are requested. I am sure all Home Secretaries take the decision very seriously and seek to come to a judgment about it. I do not know whether that sounds familiar to you, John, but that is certainly how I felt I was trying to deal with it.

Lord Reid: That is roughly the process. Obviously each individual case is somewhat different. Some are hugely different from others. Each individual case may have a different timescale. Without going into individual cases, you can imagine that, certainly on occasions, I had to deal with—I am sure Charles did, too—warrants in connection with an ongoing hostage situation, when there was an imminent threat to life. There is obviously a degree of urgency about that, and that constrains the time for consideration and, no doubt, the time for judicial review.

In Northern Ireland, lives were often plainly at risk. In those cases, you have a time constraint. In other cases, you have a pretty bulky file, sometimes on a renewal. As it happens, we had consecutive periods so, on occasions, I would have got an application to renew a warrant that perhaps had initially been okayed by Charles. Nevertheless, with duty and diligence, you would spend a bit of time going through it yourself—sometimes going through the papers that he went through. In other cases, there might be less information to be examined because it might be—for instance, in the case of an ongoing and imminent terrorist plot—that a telephone number, a name or some association had been picked up tangentially in relation to someone else that you had been looking at for some time.

The only other thing that I would say is that I suspect that, during the time that Charles and I were Home Secretary or, indeed, in any other position authorised to issue intercepts, because of the exponential rise of communication through cyber and the internet, the number of applications would be getting greater and greater.

Charles Clarke: Can I just add one point, Mr Starmer? There is an important conceptual point here, which is that modern detection of organisations which are criminal in intent—serious and organised crime, and terrorism—is basically about building up a pattern of what networks of relationships exist between different people.

You collect information, as John just implied, about particular nodes of the situation. Then the question is what forms of communication they have with others and who they are communicating with in order to try to better understand what the actual networks are and who is talking to who and, in certain circumstances, what they are actually intending to do. That is just the background that you should have in your mind when thinking about what kind of surveillance requirements are necessary to look at that.

Q247 Keir Starmer: I know there is no such thing as a typical case because they are all shapes and sizes but, in the main, would you have expected a signed statement from somebody setting out the case for necessity and proportionality—why it was necessary—and drawing your attention to the relevant material?

Lord Reid: Yes. That would be the top introduction, but there may well be further papers behind it. In some cases, there may be papers behind it in some depth.

Charles Clarke: If the question is whether there would normally—I am trying to think whether there is any exception to this—be a recommendation by an official based on the data that existed, the answer is yes. I am trying to think whether there are any exceptions to that. I cannot think of any offhand.

Q248 Peter Kyle: One of the innovations of the Bill is the double lock. When you were Home Secretaries, most warrants would have been signed just by the Home Secretary. Will the knowledge of having judicial oversight and a second authorisation before the warrant comes in change the behaviour of the Home Secretary when approaching the decision?

Charles Clarke: I tend to doubt it. Speaking for myself and, I am sure, for John—actually, for all Home Secretaries I have ever discussed this with—we have all been exceptionally aware of the severity and seriousness of what we were looking at. I do not think that the idea that there was going to be a judicial review of what we were doing would have changed our behaviour significantly. There is quite a serious, in-principle issue about the role of the judge as opposed to the role of the Executive.

I saw you taking evidence from Lord Judge just now. I bumped into him as I was coming in. The question of the relationship between the judiciary and the Executive is a key point. I gave evidence on it to the House of Lords Constitution Committee in 2007 because I think it has all been changed by the Human Rights Act 1998. I think there has been insufficient consideration of the changing nature of the relations. In response to your particular point, Mr Kyle, I do not believe that there would have been a significant change in behaviour.

Lord Reid: I do not think there will be a change in behaviour from the point of view of the person who is ultimately accountable to Parliament for the decisions, which is the elected Member and appointed Minister. Probably even before RIPA, which I think Charles took through the House of Commons, there was an awareness that there were degrees of oversight and you were working within certain constraints and certainly with oversight.

I confess that where I would worry—you would perhaps say, "Well, he would, wouldn't he? He was the Home Secretary."—is in case the judicial oversight became a co-decision. I think that is a recipe, in some cases, for obstacles to the efficient operation of aspects that I mentioned earlier, for instance in a hostage situation. I know that allowances are being made for that.

I guess that the additional oversight—judicial oversight—that is in the Bill is a result of a number of factors. One is the concern—I do not know whether it is public concern; I do not think it is, but it is certainly published concern—over the Snowden revelations, the general distrust of politicians and the fact that there was a Liberal-Conservative coalition. All of this is compromise, is it not?

I have no in-principle objections to it, provided that the first decision is made by the person accountable for it, through Parliament, to the public and the role of judicial oversight is the judicial element of it.

Q249 Joanna Cherry: On 4 November last year, when the Home Secretary introduced the draft Investigatory Powers Bill to the House of Commons, she informed us:

"the acquisition of bulk communications data, both relating to the UK and overseas…is not a new power. It will replace the power under Section 94 of the Telecommunications Act 1984".—[*Official Report*, 4 November 2015; Vol. 601, c. 971.]

May I start with you, Mr Clarke? When you were Home Secretary, how many times do you recall authorising the use of

"the power under Section 94 of the Telecommunications Act 1984"

to collect the telephone records of everybody in the UK into a single national database?

Charles Clarke: I do not recall the answer to your question at all, I am afraid; I have not prepared for this meeting, or gone back to my files, so I cannot answer the question. I think what the Home Secretary will have been trying to communicate is that the purpose of this legislation is to update legislation in the light of massive technological change, even since 1999, when I took the RIPA Bill through Parliament. As you will recall, that was to make what was being done compliant with the Human Rights Act, which required us to have a basis on which all of this was understood. Previously, this had all been done without any basis, and I was very proud to take that legislation through.

I said at the time—if you go back to the records of those hearings—that it would be necessary to update that Bill as technology moved forward, and I think that is what the Home Secretary meant in what she said. However, I apologise that I cannot give you the precise answer that you are looking for.

Q250 Joanna Cherry: Perhaps you can help me with this question. When Parliament passed the Telecommunications Act 1984, there was no such thing as itemised phone bills. Do you remember back that far?

Charles Clarke: I was hardly born then. *[Laughter.]*

Lord Reid: That is before even we were in Parliament.

Charles Clarke: Sorry. Joking aside, I understand your point completely—

Q251 Joanna Cherry: On the hypothesis that that is correct—that there was no such thing as itemised telephone bills in 1984—then the use of itemised telephone bills to compile a national phone call database could not have been foreseen when that legislation was passed by Parliament, could it?

Lord Reid: I think these are interesting questions, but they miss the point of historical change since 1984; that is the important thing. To put it at its simplest, the principles behind interception or access have always been the same, whether it was in the days when you sent a letter to somebody, or the days when you made a telephone call to somebody. The principles, put very crudely, were that if you wanted to know whose name was on the envelope, then you had a level of authority that was necessary, and oversight. If you wanted to read the letter, you had a higher level of authority that was required, normally from a Minister. Similarly, with telephone calls, if you wanted to know who was phoning whom, then you needed a level of authority that was not necessarily the Home Secretary, because after 1984 there was such information available. If, as a result of that, you wished to go into the contents of the telephone conversation, like the contents of the letter, you required an even higher level of authority by warrant.

What has changed is that it has gone from people sending pigeons, writing letters and telephoning each other, to global communication, as you will be well aware. Instead of a phone call from Cambridge to London that can be intercepted, it goes around the world in packages. Indeed, as you probably know, that is why it was produced: the internet has its origins in the necessity of protecting the command and control structure for the launch of American nuclear weapons by the American President. It makes it much more difficult to intercept that.

To put it in grossly simple terms again, somebody used to say, "We all like rabbit pie but first you have to catch the rabbit." We all want to get the needle in the haystack, but first you have to find the haystack. The problem we are all faced with now is that the haystack is global. It is global communication, which is why we get this tension between so-called bulk collection and targeted examination.

That is a long answer to your question, but I hope it goes to some of the central questions that your Committee will be asking about that relationship. Normally, a Secretary of State would authorise a targeted interception, but the explanation of why you are being asked to authorise that may relate to something much wider, as I hinted at earlier, because you have discovered the need to target this interception because of a bigger node and a bigger network.

Q252 Joanna Cherry: I was not asking about targeted interception, I was asking about the current Home Secretary's specific avowal of that fact that for many years section 94 of the Telecommunications Act 1984 has been used to collect the phone records of everyone in Britain into a single national database. I am simply interested to know whether either of you gentlemen, as former Home Secretaries, could tell us whether you had authorised that.

Charles Clarke: No, I cannot, for the reasons I have stated.

Lord Reid: You would have to ask the Secretary of State that.

Charles Clarke: I do think that the related point is future-proofing. In an area where technological change is taking place so rapidly—where you have a state of affairs on the balance between security on the one hand and liberty on the other, and where we need to keep the capacity to surveille threats to society—how do we future-proof that? That was the issue I faced with RIPA in 1999-2000, and I think it is the issue that this Committee faces in thinking about this particular piece of legislation too.

Mr Hayes: It is good to have two of my favourite former Home Secretaries here.

Charles Clarke: Name names. *[Laughter.]*

Q253 Mr Hayes: I have many favourites.

The only question I really want to ask is whether you ever felt that the test of necessity and proportionality was insufficient to allow you to make a judgment of the kind you describe? You have said that you could call for more information and that you could qualify what you had on that basis, but in your judgment, did you ever, at any point, not feel confident to make a judgment on the basis of that prevailing test of necessity and proportionality?

Charles Clarke: For myself, I can recall only one case where I felt that. In that case, I decided not to authorise the warrant that I had been requested to authorise, for exactly the reason you suggested. There was an issue in my mind about whether the proportionality issues had been properly weighed up. I think that the proportionality issues were a constant theme of any of the warrants that were sent. You had to try to make a judgment.

I cannot recall whether there were specific guidelines on this, but when I first became Home Secretary I certainly had a couple of briefing meetings about the issues in general—not about particular warrants—to try to go through some of the principles that applied. I am sure other colleagues did much the same. I do not recall a written-down document that tried to explain the proportionality judgment in general, because obviously in reality you are always making the proportionality judgment in particular cases. My approach was that if I did not feel it was satisfactory, I would not agree the warrant.

Lord Reid: I take it that you are asking, "Were there occasions on which you refused a warrant because you didn't think it was either proportionate, sufficient or necessary?"

Q254 Mr Hayes: Yes. Obviously you know, as you are very familiar with it, that that is the kind of baseline requirement. I presume that the case that was made to you was mindful of that requirement and that, for the most part, you felt it met the requirement. I just wanted confirmation of that.

Lord Reid: To give you a straight answer, yes. When I was Home Secretary, I refused a warrant. On other occasions, I refused to renew a warrant. I cannot remember specific cases in Northern Ireland, but I did it there as well. In the first instance, when a warrant is put to you, you are exercising a degree of judgment. And very often you are exercising a judgment based on other people's judgment, and their judgment is often based on fragmentary evidence. That is the problem with all intelligence, as we know to our cost in some cases. You exercise a judgment, and that judgment is hopefully exercised diligently on the criteria: "Is this proportionate? Is it necessary? Is it reasonable? What is being asked here?" There were occasions on which the answer was no. Before you said no, the normal process would be to call in the various officials—the people who put the submission to you—if necessary, and to go through it orally and ask them questions. The answer to your question of whether I ever refused a warrant is yes.

Q255 Byron Davies: You have answered the main question I was going to ask, but this is carrying on from that. Times have moved on since your days in the Home Office in terms of technology, with smartphones, et cetera. If you were sat in the Home Office now, would you be looking at introducing this Bill?

Lord Reid: I don't think it is entirely up to the Home Secretary to introduce it. There are two countervailing pressures. One is the development of cyber, which is something that, having stepped down from the Cabinet, I have voluntarily spent a lot of time working on. By the time you get this Bill through, in whatever form, we will

[Byron Davies]

no doubt be faced with artificial intelligence and a whole new era of communication. Yes, it would be necessary to take into account the changes, as I was saying to Ms Cherry earlier, in the world of cyber, and particularly the global nature of communications.

Secondly, there are undoubted pressures from the other end, not just the wish from the intelligence services and the policing side. I don't think their motives and objectives have changed; what has changed is the world around them. Therefore, to meet the same objectives, they have to employ different methods on the old principles. However, at the same time, I am well aware that there has been widespread—"discussion" is a very light word—controversy about access to people's information. Sometimes it is a paradox, because people are willing to supply all sorts of information to all sorts of private companies. That information is not only being put in a databank but is being mined, matched, sold and used for commercial reasons. Nevertheless, whatever the paradox, the concern is there, and I think the Bill tries to meet the needs of addressing technological change on the side of security at the same time as giving the reassurances necessary because of the public's concerns about the new world in which we live and about intervention into it. That is against a background where, as the Committee will know, one of the constant characteristics of the world of cyber and communications is constant entrepreneurial innovation by black hats and white hats. It is literally changing every day. Therefore, the equivalent of today's microdot, where we used to put secret messages, can be a webpage—an apparently innocent webpage that can be sending all sorts of instructions, propaganda or whatever. There are very bright people in both the black hats and the white hats who are constantly inventing things, vis-à-vis each other.

The Chair: We really are pressed for time, gentleman. Can we have shorter answers so I can get as many colleagues in as possible?

Charles Clarke: My short answer is yes, I would have been in favour of introducing such a Bill. I think the question of updating with future-proofing is very important. On the timing, I cannot comment on whether the Home Secretary was right to introduce it now as opposed to in five years, or five years before, or whatever. The only factor that I would add to John's remarks is that the capacity of the organisations that we are trying to contest is a very important issue and they are very wealthy, very effective, very scientific and very powerful, as John said. An assessment will be being made, which I am not privy to now, of how effective those organisations are now, which undoubtedly would have informed the Home Secretary.

Q256 Victoria Atkins: I have one question for Mr Clarke. You were the Home Secretary during the 7/7 bombings. How important was your experience of warrantry and your relationship with the security services in the hours and days that followed that terrible event?

Charles Clarke: Critically important. I believe that one of our strengths in the UK is that we have good relations between the different security services, the police and the political establishment in these areas. Indeed, with 7/7 itself, there had been substantial rehearsals of the various co-operations that needed to take place. I think that co-operation between the various agencies charged with the security of the country is exceptionally important, and 7/7 reinforced that for me very much.

Q257 Victoria Atkins: When you were standing up in the House of Commons at the Dispatch Box explaining what the security services and the police were doing, how important was your personal oversight of that, as opposed to just a judge doing it by themselves?

Charles Clarke: The implication of your point I could not agree with more. My personal experience was very important. It did lead me, personally, directly to have relations with the individuals in the security services who were involved with these things, and I think that helped my whole job as Home Secretary.

Q258 Matt Warman: You talked about updating the legislation and the importance of that. Do you see an internet connection record or something equivalent to it as a key part of updating this legislation for the world we live in now?

Charles Clarke: I do personally, yes.

Lord Reid: I do as well. Not to test the Committee, but two years after 7/7, on 6 August 2006, there was a plot to bring down seven airliners. There would have been 2,500 victims, and intercept was absolutely essential in protecting those lives—absolutely essential—with both the internet and telephone communications.

Q259 Suella Fernandes: It has been raised before, but some witnesses have said that warrantry should be solely within the Executive function—

Lord Reid: What, sorry?

Suella Fernandes: Warrantry should be retained by the Executive. Other witnesses have said that it should be a judicial function. The double lock is a middle way. Where do you both sit on that spectrum, ideally?

Charles Clarke: Personally, I am in favour of the Executive responsibility. I would prefer to have that. I think the more you draw the judiciary directly into the operation of the law, as in continental systems, the more you threaten the ability of the judiciary to play its characteristic role. I understand why proposals are being made to have a double system, and I am not against it, but it is against my instincts, actually. It is a path that has been ill thought through. There is a whole section of lobbies in this country who believe, essentially, that the lawyers are better people, in whom you can have more confidence than in the politicians. I reject that assessment.

Lord Reid: I agree entirely with Charles on that. I think that there are a couple of other reasons as well. First, this judgment ultimately is not just the strict codification of a law, although it involves that; it is about political judgment—I therefore think that there is a second reason. The third reason is quite simple. If a wrong decision is made and 2,500 lives are lost, for instance, it will not be the judges who are held accountable—I do not just mean by Parliament, but by the family, the public, the community—it will be the Minister. Therefore, for those three reasons, I personally am in favour of this being the decision of the Executive. For the reasons that I explained, I am willing to accept

that the Home Secretary has had to bow to other pressures and to put in judicial oversight, but only as long as that is about oversight and judicial process, and not about decision making. If it is about decision making, I think it is a recipe for ineffective operational capability.

The Chair: I thank our two witnesses for tailoring their responses in a way that allowed all colleagues to get in, including Back-Bench colleagues. Absolutely fascinating. On behalf of the Committee, I wish you a very happy Easter. Thank you so much for being so generous with your time.

5 pm

The Chair adjourned the Committee without Question put (Standing Order No. 88).

Adjourned till Tuesday 12 April at twenty-five minutes past Nine o'clock.

Written evidence to be reported to the House

IPB 01 Muslim Council of Britain

IPB 02 Willie Mckenna

IPB 03 David Sawford

IPB 04 John Bingham

IPB 05 Jaron Shulver

IPB 06 Dr Paul Bernal, Lecturer in Information Technology, Intellectual Property and Media Law at the UEA Law School

IPB 07 Guardian News & Media

IPB 08 Brass Horn Communications

IPB 09 Brian Scallan

IPB 10 David Mytton

IPB 11 Martin Kleppmann

IPB 12 Keith Alexander Mallen

IPB 13 Adrian Kennard

IPB 14 Information Commissioner

IPB 15 Tirath Bansal, Director, Myorb Limited

IPB 16 Annie Machon

IPB 17 Maritime and Coastguard Agency

IPB 18 James Le Cuirot

IPB 19 Scottish PEN

IPB 20 IT-Political Association of Denmark

IPB 21 Apple, Facebook, Google, Microsoft, Twitter and Yahoo

IPB 22 Chief Inspector Keith Conradi, Air Accidents Investigation Branch, Chief Inspector Steve Clinch, Marine Accident Investigation Branch, and Chief Inspector Simon French, Rail Accident Investigation Branch

IPB 23 Open Intelligence

IPB 24 Stuart Johnson, Director, Logic Ethos Ltd.

IPB 25 Big Brother Watch

IPB 26 News Media Association

IPB 27 techUK

IPB 28 Criminal Cases Review Commission

IPB 29 Leonard J. Crabs, on behalf of the Megan Kyanka College Fund

IPB 30 Ray Corrigan

IPB 31 Internet Service Providers Association

IPB 32 Bingham Centre for the Rule of Law

IPB 33 Digital-Trust, CIC

IPB 34 Equality and Human Rights Commission

IPB 35 Christopher Lloyd

IPB 36 Center for Democracy & Technology

IPB 37 Kevin Cahill

IPB 38 Bar Council

IPB 39 Justice