HOUSES OF PARLIAMENT

Joint Committee on the Draft Investigatory Powers Bill

Oral evidence: Draft Investigatory Powers Bill, HC 651

Wednesday 6 January 2016

Watch the meeting

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

Questions 224 - 258

Witness: **Christopher Graham**, Information Commissioner, gave evidence.

Q224 The Chairman: Welcome, Mr Graham, and thank you for coming along to talk to us this afternoon, so soon after the new year, when we are just starting up politically. As you know, this is an extremely important Bill, which is going through both Houses. We have been charged with the task of pre-legislative scrutiny. You undoubtedly have significant views on the issues that are in front of Parliament. I am going to kick off, if that is okay, with a rather general question to you. If you wish to add some comments more generally, we would be delighted to hear them. Thank you again for coming along. My question is: do you think that the draft Bill is actually necessary, from your point of view, and does it strike a balance between privacy and security—the age-old balance between those two things?

Christopher Graham: Good afternoon, Lord Chairman, and thank you for inviting me to contribute to your deliberations. I know that you are having to work very fast on a very complicated Bill; I counted nine parts, 202 clauses and nine schedules and I think that you have to report back to Parliament very speedily.

To answer your question, some legislation is clearly necessary, because the previous legislation was struck down by the courts. Indeed, the fundamental question about necessity and proportionality is still before the Court of Justice of the European Union. Nevertheless, following the reports from David Anderson and RUSI, suggestions were made for making much clearer and much more explicit what the proposals for the use of data are and what the procedures and safeguards should be. I suppose that this Bill is a response to that.

It is very difficult to judge whether the Bill gets the balance right between security and privacy. The one thing that we do not have in the voluminous material that has been put before you is any real evidence, as opposed to the occasional anecdote, on the utility of the

information that is sought. The Bill proposes that data can be required to be retained for 12 months, but there is no particular explanation of why 12 months rather than six months or 18 months is desirable, because there is no indication of the use that such information is being put to over many months and years in the normal way of dealing with serious crime and terrorism.

All that I would say as Information Commissioner, in answer to that point, is that Parliament needs to see this in the context of the way the digital world works. Whatever we do, we are all leaving a trail of information, but we also have rights, under the data protection directive and the Data Protection Act, to have our privacy respected. There needs to be a balance between the common interest in security and the individual interest certainly, although I would also say the common interest in privacy and an acceptance by Parliament that data protection is a fundamental right under the Charter of Fundamental Rights of the European Union. I do not think that it is a question of just signing a blank cheque. I would be very much in favour of Parliament continuing to stay with this issue and, after the legislation is passed, as I suppose it will be, making sure that it returns to the issue time and again to make sure that the information that is being retained and exploited is being used properly and that the use is proportionate, needful and helpful.

Q225 The Chairman: Thank you. In your written evidence you said something that the Committee found very interesting about the question of a possible sunset clause in the legislation. Perhaps you could expand a little on your views on that.

Christopher Graham: This develops the point that I was just making—the proof of the pudding, Lord Chairman. It is asserted that this information is very important for the prevention and detection of crime and terrorism. I think that it would be sensible and wise for Parliament to review from time to time how it is working in practice. What use is being made of this great mass of data that will be required to be retained by communications service providers? Did it actually contribute? There is a huge risk, with all that information being retained that otherwise would not be, that that information could be exploited by bad actors, so there are security challenges for communications service providers. Parliament would need to be convinced that the case that had been made was working out in practice. After all, Parliament renewed the Prevention of Terrorism Act year by year, so I cannot see why we should not have a similar arrangement for something so fundamental as this Bill.

The Chairman: Would you see that as being an annual review or a bit longer than that?

Christopher Graham: Well, Parliament managed to do an annual review of the Prevention of Terrorism Act and took it in its stride. That was when life was a little simpler. We have to bear in mind that if we are saying to communications service providers, "We want you to retain everything for a year and then, under a system of warrants, we reserve the right to look at it", we are building up a risk around data security and privacy. Parliament has to be pretty sure that that remains justified and that the arrangements remain secure. One way of doing that is to have a sort of rolling sunset arrangement.

Q226 Lord Strasburger: Good afternoon. One sentence in your written submission caught my eyes. In paragraph 7, you say, "there is an increasing danger that we are living in a society where few aspects of our daily private lives are beyond the reach of the state. This

poses a real and increasing risk that the relationship between the citizen and the state is changed irreversibly and for the worse". What did you mean by that?

Christopher Graham: What I meant was that simply by the fact that we are all doing business, social interaction and communications digitally, wherever we go and whatever we know, like it or not, we leave a digital trail. The challenge for a data protection framework is to make sure that that remains private where it should be private or, if it is accessed and shared, it is accessed and shared within a regime of data protection where all the rules are agreed. What I am not prepared to sign up to is the suggestion that willy-nilly the state ultimately always has a right to access all that stuff, just because (a) it can and (b) "Salus populi est suprema lex", and all that. The case has to be made constantly for the necessity and proportionality of anything that invades our privacy, whether it is a commercial invasion, whether it is by state agencies, whether it is information sharing within the health service or whether it is information to keep us all safe and secure in the face of terrorist threats. I am not pretending that that challenge is not there; I am just saying that we have always to be clear that the rules under which that information is accessed have integrity and are closely followed. The fact that the state and commercial entities can have access, physically, to this material is obvious; the question is under what regime they should be allowed access in a good cause.

Q227 Mr David Hanson: In your written evidence—and you have touched on it again verbally today—you indicated that you think there is little justification being advanced for the 12-month retention period. Ultimately, do you think that the 12-month retention period is correct or not?

Christopher Graham: When I say that little justification has been advanced, I mean that those who are putting forward this Bill are not explaining what 12 months is about—why 12 months? If you are going to say, "We reserve the right to invade your privacy, and by the way this material has to be retained for 12 months", you have to make the case for that. Nowhere in the Bill or supporting memoranda have I seen the argument for 12 months. It is not for me to say that I think 12 months is wrong or right or that some other figure is appropriate because I am not the one seeking the powers; I am not the one who knows what we want to do with the information; I am not the one who knows how the information has been used. I am realistic; I understand that there has to be some care with which the facts are bruited abroad but nevertheless, nowhere in this 296-page package is the case actually made for 12 months.

Mr David Hanson: We have received evidence from police and other agencies that there are long, drawn-out investigations where serious crimes are potentially being committed, or have been committed, where the 12-month retention period is required. If that case were made by the Home Secretary and/or the agencies, you have no objection in principle to the 12-month period as opposed to a shorter or longer period?

Christopher Graham: I do not know what advice you have seen; as I say, it is not in the 296-page pack. But I would be a little wary if there was one anecdote—one case, I apologise—where information that was 12 months old was useful. I would still take some persuading that that justified the retention, potentially, of everybody's everything for 12 months, just in case.

Q228 Dr Andrew Murrison: Good afternoon. In your evidence you suggest that there might be a stronger role for the Information Commissioner in auditing communication data. I would be interested to know what you mean by auditing and what exactly you would be checking up on. Would it be the kinds of data sets that have been gathered or the way that they are stored and managed, or the way that they are used by the authorities?

Christopher Graham: To be clear, I am talking about the role of the Information Commissioner under this Bill being very similar to the role that we have under DRIPA and the Data Retention Regulations, which is not to make judgments about whether or not information should have been used in the way that it was used but based simply on the data protection principles of making sure that information that is retained which otherwise would not be is retained securely, is not inappropriately accessed by people who have no business to see it, is not leaked and does not go AWOL, and that it is also securely deleted at the end of the specified period. My good practice team and my expert auditors are engaged in that process and I imagine that under these proposals they would continue with that sort of work.

To do that, I could do with a few improvements to the Bill, if I may. I have obligations as the Information Commissioner under the existing legislation to audit communications service providers and to make sure that information is secure and is appropriately deleted. But the communications service providers do not seem to have any very specific obligation to co-operate with me. I am not saying that they do not co-operate but it takes an awfully long time to get in to see the communications service providers. I would like to see that not left to codes of practice but in the Bill.

I think it would also be a reassurance to those communications service providers if they were absolutely confident regarding the same obligations that my staff have under the Data Protection Act to keep secure the information that we receive in the course of an investigation; Section 59 of the Data Protection Act carries a criminal sanction if I or any of my staff abuse our position. That should be explicitly extended to the obligations on the communications service providers under this legislation so that they have the confidence that any information they share with me and my staff will be respected under pain of criminal sanction. I make this point because we are wasting an awful lot of time sending auditors on to sites to spend three days reading up all the material; if we could see it in advance, we could prepare and just turn up and do an audit based on the questions that arise from the material. Those are very practical points which would make the job of the Information Commissioner a lot easier and probably the ICO easier to deal with for the communications service providers.

But you ask about the use of the materials retained, and that is just not my territory. That is not what I am asked to do. You have had evidence from the distinguished commissioners who labour in that particular vineyard. I think I said in my initial remarks that I cannot make that assessment. I just do not know how that information is used and whether it is used appropriately. If Parliament is relying on me to answer those hard questions, you need a better structure in place for dealing with it, which is why I suggested post-legislative scrutiny, sunset clauses, and so on.

Dr Andrew Murrison: Do you think that those who drafted the Bill struggled with putting obligations on CSPs which they could not then enforce? The last thing we want is a law that

is unenforceable and could be waived by authorities outwith the territory of the United Kingdom, for example.

Christopher Graham: I think that all the communications service providers want to co-operate as best they can. I have seen the suggestion that some of them are worried that if they accept the principle of extraterritoriality in the case of the United Kingdom, they might be required to do the same for the Chinese or the North Koreans. I do not detect any reluctance to co-operate sensibly. But the fact is that under the present legislation—DRIPA—my statutory obligation to carry out the audits of security and timely deletion is seen by communications service providers as just another regulator doing what regulators do, and I need that more specific legal power to make sure that we crack on with things in a business-like way.

Q229 Stuart C McDonald: Mr Graham, you have already referred several times to the importance of the security of retained data. Based on your experience of auditing communications service providers' retained data, how much faith can we and the public at large have in the security arrangements that they have in place for retained data?

Christopher Graham: We have been charged with that responsibility under DRIPA only over the past couple of years or so. We have managed to get round the major communications service providers in the UK. I would have liked to have been able to do it faster. As I said, perhaps the communications service providers did not have the same sense of urgency that we had, but nevertheless we have got round the communications service providers. We have not found things that shocked us, I will put it that way. Under this legislation it will be very important to continue to make sure that arrangements are in place for the secure retention of data. We had concerns about data perhaps being housed with other data that would be accessed in the normal course of business and it probably was not a good idea to have those two data sets held side by side. We are very keen to engage with the communications service providers to make this system work.

Stuart C McDonald: Are the service providers quite co-operative in resolving that sort of issue if you raise it with them?

Christopher Graham: Yes, our problem has really been a scheduling one; unless I have the statutory power to say, "I am sorry, I am not asking, I am telling: I am coming", the answer will always be, "It is not really convenient. We will see you in three months' time. Oh dear, that is not convenient either. We will see you in another three months' time", and so on. I want the explicit power in the Bill to be able to go in and audit communications service providers in the same way that I can with government departments or health service bodies. This is really important. If you are saying that the nation's communications data is going to be held under some circumstances or even most circumstances, where it otherwise would not be, the regulator has to be given the powers to make sure that that is actually being done properly: that the information is being held securely and when it is dealt with it is gone.

Stuart C McDonald: From what you said, you have not had the opportunity yet to look at some of the smaller service providers and the security of the information that they retain.

Christopher Graham: Yes, it has been fairly slow work but we will continue with that whether or not the Bill goes through.

Stuart C McDonald: You have spoken about co-operation a couple of times. I sense that it is not so much a complete lack of co-operation but just a lack of priority or urgency on their part.

Christopher Graham: Yes, "lack of priority or urgency" is a fair way to characterise it.

Stuart C McDonald: What involvement do you have with overseas-based service providers and what is your relationship like with them?

Christopher Graham: We have a good relationship. Some of the big players, of course, are based elsewhere. But as the UK data protection authority, we are dealing with these players all the time. We usually have a pretty good working relationship with them and we will see how this legislation works out.

Stuart C McDonald: So you do not notice a difference between overseas-based providers and UK-based providers? Is there roughly the same level of co-operation?

Christopher Graham: The same level of co-operation, I would say, yes.

Stuart C McDonald: You also have experience of auditing the information-handling practices of police forces. Again, how much faith can we have in the security of the information and data that they retain?

Christopher Graham: We have been auditing police forces for years under the Data Protection Act and the Privacy and Electronic Communications Regulations. We have audited 40 forces. Again, this is a consensual audit—I do not have the power of mandatory audit—but again we have not had a single audit where the conclusion has been "very limited assurance". Breaking down those 40, we have had two that came in at "high assurance", 24 that came in at "reasonable assurance", and 14 that came in at "limited assurance". Where it is limited assurance, we have a checklist of the things we want the force to do before we go and see it again. The police service is very much engaged with the data protection and security issue. We are talking to them all the time and working with the national police improvement people—formerly, ACPO—and I am reasonably confident that we have a good working relationship with the police. Again, what I cannot judge is what use the police are making of retained material.

Stuart C McDonald: Sure. Indeed, there was a news story just a couple of days ago about the completely inappropriate use of retained material by one or two rogue officers. There has to be a limit to what you can achieve. You can never do anything more than make sure that appropriate systems are in place. You cannot ensure that an individual officer is not going to go rogue, as it were. Can systems be put in place to try to stop that sort of access to information?

Christopher Graham: There is the criminal sanction in Section 55 of the Data Protection Act. I might wish that Parliament could persuade Ministers to activate a greater deterrent penalty; at the moment, it is a fine-only regime. Of course, Parliament passed legislation to enable the possibility of a prison sentence but it has never been commenced. That is

something the Committee could recommend. We do act when individual officers go rogue. It merely underlines the point that when you require communications service providers to retain a massive collection of data for a year, it creates a risk. It is there. People may do stupid things with it. The Committee should not concentrate simply on whether or not use by the forces of law and order is appropriate and appropriately warranted; it is also just a whole pile of stuff that can get lost or inappropriately accessed from a criminal point of view and so on. Because that risk is created by the legislation, you have to have some very powerful safeguards to make sure that the legislation is reviewed regularly, that it is being used for what it is meant to be used for, that it does what it says on the tin, and so on.

Stuart C McDonald: Finally, do you have involvement in auditing the information-handling practices of the intelligence agencies? If so, what faith should we have in the security of the information that they retain?

Christopher Graham: No, I am not invited to that particular party.

Q230 Suella Fernandes: Good afternoon. I have a simple question, if there is such a thing. There is an issue around when privacy rights are engaged and I wanted to get your perspective on when you think those rights arise. Does an intrusion occur when information has been read? Is it when it has been analysed or subjected to automated filtering or to human examination? What is your perspective?

Christopher Graham: The risks and the rights arise at the point of collection. It is a fundamental data-protection principle under the directive from which the Data Protection Act arises that information is not retained for longer than is necessary. If you create the requirement for information to be retained, that calls into question the obligation under the seventh principle, that personal information must be secure. The very first principle – that personal information must be fairly and lawfully processed – arises when the profiling of individuals takes place based on the information that has been retained, and decisions are taken about individuals that may be to their disadvantage that have nothing to do with law and order or security but are just about treating people differently because of information that you have been able to get hold of. So I would not subscribe to the view that it is a question only of deciding on the proportionality and necessity of looking at particular pieces of information because we have reason to believe that so and so is up to no good. I do not oppose that at all. I am just saying that information rights are impacted and a risk is created simply by the amassing of this huge amount of personal information, which may or may not be needed for the purposes that it was originally collected for.

Q231 Lord Hart of Chilton: Good afternoon, Mr Graham. You say in your written evidence: "Examples of the need for bulk personal data set warrants are not persuasive since equivalent provisions already exist in statute. The established approach could be used for data sets of concern. Consideration should be given to exempting certain data sets involving sensitive personal data, such as those, for example, relating to health data". How would the provisions of the draft Bill alter the range of these data sets, and how would you like to see the Bill amended to provide the audit arrangements that you say are necessary?

Christopher Graham: The point that I was making was that in the Explanatory Memorandum—the guide to powers and safeguards—the authors of the Bill have chosen some very inapt examples of the sorts of bulk data sets they want to access for reasons of law and order, by giving the telephone directory and the electoral register as the two examples. This is bizarre, because that information is already available. Explicitly,

legislation was amended to make sure that that information is available to the security services. It does not require this Bill to provide that. That begs the question of what are these data sets that are so necessary, and we are not told, which then begs the question that if the authorities are not going to tell us what data sets they are going to be accessing, are they prepared to say what data sets they would not be prepared to access?

There is very great public concern about various initiatives in the health sector around the care.data project. Patients were very concerned that their most personal and most sensitive information was going to be uploaded into a health service information centre and then shared around rather freely with the insurance companies and heaven knows what. People were very concerned about that. That scheme has now been rethought and that is very good news. But are we being invited to give a blank cheque to the authorities to access everyone's most sensitive health data? I suspect not, but it does not say that in either the legislation or the guide to powers and safeguards. It seems to me that they picked a silly example, because you can already access the electoral register and the phone book, but there is some reticence about talking about what would be off-limits.

Lord Hart of Chilton: Earlier, you gave some examples of how you would like amendments to be made. Do you have any amendments you would like to be made here?

Christopher Graham: I would probably stick to the job that I am charged with, which is inviting the Committee to consider specific amendments to those statutory obligations I am under about the auditing work under the Bill that we are specifically asked to do. I have two roles here: one is to make the general point about the balance between security and privacy, which of course has also been made by others in evidence to you; the second is dealing with the specific powers and duties of the Information Commissioner under this legislation relating to the auditing of retention and deletion by communications service providers. I think I will probably stick to that, if I may.

Q232 The Chairman: It has been argued that the revelation of details of further data sets could damage the work of the security services. Do you think they have a point?

Christopher Graham: That is the eternal dilemma of this subject. I have been Information Commissioner for six and a half years, and before I even took up the post I was being approached by the Home Secretary to understand the absolute importance of what was then going to be the communications data Bill. It is very difficult to get the rules right, and I understand that security services and the police find it difficult to be explicit, because it gives the game away to bad actors. The trouble is that the Anderson report last year and the RUSI report called for an end to obfuscation and secrecy, and said that we must have transparency to win public confidence. The Home Office should probably be more forthcoming about what it is talking about here. We seem to be a bit betwixt and between—more transparent than we were, but not quite transparent enough to win the argument.

Q233 Bishop of Chester: It is good to see you in this context. It falls to the bishop, for some reason, to talk about oversight and how it works in these contexts. You said that the new IP commissioner "must be independent and inspire public confidence". Do you think the draft Bill is framed in a way that will promote that?

Christopher Graham: Well, clearly there is a lot riding on the new commissioner. The way in which the commissioner is appointed will be key. As a commissioner myself, the resources that the commissioner has to do the job will also be very important. You can have high-sounding powers and responsibilities but if you do not have the resources and people to carry them out, that will be a complication. We have done a lot of work at the Information Commissioner's office working with the various Home Office commissioners to try and make it clearer to the outside world how the regulatory framework goes. At my initiative, the various commissioners published a road map of surveillance, so that individuals could see who was doing what. We work very closely together. We are working on a memorandum of understanding with the Interception of Communications Commissioner, in particular on the reporting obligations for communications service providers to make sure that they need tell us only once, in effect, and then it is up to the two commissioners' offices to work together to make sure that the right people get to know what they said.

Primarily, in my experience, commissioners are judged by the way in which they perform. Obviously, commissioners will be expected to appear before parliamentary Committees and so forth. A commissioner will be expected to report regularly. Clearly, the Interception of Communications Commissioner's office is an exemplar of how that should be done at the moment. Fundamentally, is Parliament or the Home Office going to vote the funds to enable the new commissioner to do a proper job?

Bishop of Chester: What is it about your present role that you think really promotes your own sense of independence as the Information Commissioner, and the public confidence that there clearly needs to be in your role, too? What is the key thing that supports those features of your role which should potentially transfer to the new role?

Christopher Graham: I am tempted to say to the Bishop of Chester, "Not being based in London", but it might be fanciful to think that this commissioner will be based in Wilmslow or anywhere similar. It is not a trivial point: there is some advantage in being just a little bit distant from the centres of power and influence in Westminster. Otherwise, it is a question of having the resources to do the job. I am funded by the levy that all data controllers pay. Many £35s add up to the best part of £18 million or £19 million, so my office is very well resourced. I hope the new commissioner will be similarly resourced, at least in the sense of adequately, though I suspect that would more likely be by grant in aid from the Home Office. This is an important area. It must be properly funded.

Bishop of Chester: We have been discussing how the funding regime would work for this. Are you content with how your role will relate to the new commissioner's? Do you feel comfortable with how that would be set up?

Christopher Graham: We have to make it work. As I said, it was at my initiative that I got together with all the Home Office commissioners and also the Surveillance Camera Commissioner and the Biometrics Commissioner. We had very regular meetings and produced that road map. We are working on a memorandum of understanding to make sure that we do not cause aggravation to communications service providers by asking the same set of questions twice. It is all in the co-ordination. I do not think that it requires a culling of commissioners—though I would say that—but co-operation between them, certainly.

Bishop of Chester: So are you satisfied with how it is set up to relate to your office, broadly?

Christopher Graham: Yes, we will do our little bit, but it is a little bit of the whole surveillance and security piece, which is a little bit of the whole data protection universe. That is what we are concerned with.

Bishop of Chester: One of the issues for independence is how the roles of authorising interception and overseeing what has been done relate to each other. There have been some suggestions that the commissioners could be like people who mark their own homework: that the same body will, as it were, both authorise warrants and exercise an oversight of that process. Is there a case for greater separation somehow between those two roles with the IP commissioners?

Christopher Graham: On reading the transcript of the session on 2 December, when you asked that question, I was rather sympathetic to the point you made about the nature of a double lock. It did not feel much like a double lock to me, more like a conflict of interest.

Bishop of Chester: Should it be a triple lock—in other words, by separating the oversight role from the authorising role?

Christopher Graham: I hesitate to go there. David Anderson originally suggested the clear involvement of the judiciary in the authorisation. My reading of his evidence at the 2 December session was that he seemed quite happy with what had been proposed. I just do not know; all that I am saying is that if, in my office, I had responsibility for one set of people authorising something and another set of people deciding whether they should have authorised it, I would find that slightly odd.

The Chairman: Mr Graham, thank you very much indeed: that was an extremely useful and informative session. Thank you for coming along.

Witnesses: **Jesper Lund**, Chairman, the Danish IT Political Association, and **William E Binney**, retired Technical Director of the United States National Security Agency

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

William E Binney: First, I thank the Committee for giving me the opportunity to come and give testimony. I hope I can help you with some of the issues you are discussing in this Committee. My big objection with how NSA, GCHQ and the law-enforcement agencies affiliated with them deal with data is fundamentally about the bulk acquisition of

data of any type. When I became the technical director of the world analysis and reporting group at NSA, which had about 6,000 analysts and was responsible for reporting on every country in the world, I had to look at the major problems that they were facing and try to figure out ways of solving them. I took the position in 1997, when the big explosion of digital communications was occurring, so the biggest issue I had to face was that explosion and how our NSA analysts were dealing with it. This was also true at GCHQ. GCHQ and NSA basically do the same thing, so they co-operate very closely. If one has a problem, the other does, and they have the same problems. The issue was that our analysts, even back then in the 1990s, could not see how to resolve issues around the world because there was too much data for them even to look at. That was before we had the bulk acquisition of data we have today. Back then, we were collecting the smallest lines of communication. We could not deal with the fibre rates. We did not invent that. A little lab I had, the Signals Intelligence Automation Research Center, invented the ability to pull back together and recompile everything going at fibre rates in 1998. At that point, we deployed that, creating problems that were orders of magnitude greater for the same analysts because they were still doing dictionary select routines that would look through data and pull out anything that matched the dictionary. That basically pulled in everything, dumping all that data on the analysts, so they could not see the forest for the trees.

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

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

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

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

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

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

Q236 Suella Fernandes: I want to look at the comparisons between the Danish experience and what is proposed in this Bill. Mr Lund mentioned cost. Would you agree that one of the big differences was that in Denmark the equipment cost of data retention was borne solely by

the communications service providers, whereas there is a very different approach under what is proposed in this legislation?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

haystack, whereas presumably the information that can be obtained by seizing the suspect's laptop or smart phone and searching that is of much better quality for the police investigation.

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

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

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

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

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

Jesper Lund: No, I am not.

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

Jesper Lund: Danish communications providers follow the law, of course. They also work together with the Government on setting up systems that are manageable. So the history of the Danish system for the collection of internet connection records was not just a matter of cost; it was initially a matter of the Minister of Justice wanting something that was technically unfeasible. I see signs of the same thing in this Bill. For instance, it is mentioned that an internet connection record could be the destination IP address or the server name. It is certainly possible to define internet connection records in terms of both IP addresses and server names but, in terms of complexity, and hence of the cost of running these systems, there is an order of magnitude in the difference between requiring communications service providers to retain the internet protocol address and doing the

same for the server name. The first is pretty simple, but asking them to retain the server name is asking them to do deep packet inspection because the server name is not really available to them. What they get is a packet and an IP address, and then they transmit that packet to the IP address. To get the server name they will need to do some form of deep packet inspection, which is a lot more costly than simply retaining the server name. There was collaboration between the Danish telecommunication industry and the Ministry of Justice, to the benefit of both parties.

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

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

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

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

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

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

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

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

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

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

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

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

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

William E Binney: Currently, there is not too much of a balance unless there is an attack, for example the recent attacks in Paris. Take those two attacks as the case in point. After the first attack, they went to bulk acquisition. How much good did that do them in helping to prevent the second attack? It did not help, but they started getting and finding people once they found out who did the attack and focusing in on the data they already had

accumulated on those people, which they could have got originally from a targeted approach upfront instead of waiting. By doing that, now they find other people and are potentially stopping future attacks.

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

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

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

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

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

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

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

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

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

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

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

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

Victoria Atkins: What is this document?

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

Victoria Atkins: Is it a computer program?

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

Victoria Atkins: And who owns it?

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

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

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

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

William E Binney: I guess I am.

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

Jesper Lund: Yes

Shabana Mahmood: So the argument is that the Danish example is not helpful because there was this whole bunch of data that could not be accessed and therefore it does not tell us anything about what we are trying to do with internet connection records in this country. But is it not the case that even if in the Danish experience they had been able to get that 50% of smartphone data and had complete coverage, as our system attempts to do, that data would have been potentially mostly useless because of the problem of constant connection and the fact that on smartphones the apps that police and other people would be most interested in are

on a background app refresh and therefore constantly connected to the internet, which tells you nothing about when it has been activated? Would you agree with that?

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

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

Jesper Lund: It is always hard to make statements about hypothetical situations, but I would still say that if there was a rational case for using internet connection records, Danish law enforcement should have been able to prove that using the other half of the customers, where these limitations were not a problem.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Matt Warman: But that is not what is in this Bill and not what we are talking about today. PRISM is fundamentally different. This is not a Bill that proposes PRISM.

William E Binney: No, but PRISM is an analogy to filtering because it filters too.

Q245 Lord Strasburger: The common factor between just about every successful terrorist attack in Europe over the past 10 or 15 years has been that one or more of the perpetrators was known in advance. Are you saying that attacks such as 9/11 and 7/7 could have been stopped if the agencies had used smart collection instead of grabbing absolutely every bit of data that went by?

William E Binney: Yes. In fact, in the case of 9/11, Tom Drake, who took over the efforts that I started with Ed Loomis to do a targeted approach, took the program and ran it against the entire NSA database in February 2002, very shortly after the attack, with the knowledge that we had prior to 9/11 incorporated in it. That program pulled out all the data that was in the database that NSA did not know it had on the terrorists prior to 9/11, so it gave them all the alerts, all the phone calls to the Yemen facility, all the phone calls back to Hamburg and to Afghanistan, even all the internal relationships, and showed all the data about who was involved in the attack prior to the attack. That would have alerted them. The difference was that we were putting in automated algorithms so that when they hit something of interest and we knew it was of interest, the program automatically executed. There were no people involved in that decision. So the program would alert everybody electronically and pass reports to everybody who needed to know once something was detected. It was done in an automated software way. We did not have the impediment of having people look into databases to find what was important in the data and so on. That would have at least alerted people and given them the opportunity to stop 9/11. The same is true with all the other attacks because all these people were known and in knowledge bases already. If the agencies had done a targeted approach from the beginning and kept the data finite, their analysts could have found the threats. That is my point.

Q246 Stuart C McDonald: Turning again to internet connection records, we have heard Mr Lund's views about their practical utility. Mr Binney, if this Bill is passed, can you see internet connection records being of practical use to law enforcement and to security and intelligence services?

William E Binney: Not in the bulk collection way, no, because again you have the same problem: if you take in hundreds of millions of records, you have to have people looking through hundreds of millions of records to find what is important. That is why the White House issued the Big Data Initiative in early 2012, soliciting corporations to come up with algorithms that would find information in big data that was important to look at. They issued that initiative because they have this problem, too.

Stuart C McDonald: I can see that from a security intelligence point of view, but I turn to a law enforcement point of view. One example that law enforcement gives us is missing persons. They say that because telephone records are pretty hopeless, they would love to have access to a missing person's internet connection records to see whom they have been communicating with. There are cases where they could have tracked a missing person more quickly if they had had the ability to do that. Do you recognise that as something that could be helpful?

William E Binney: Yes, and they can do that in a warranted, targeted approach. ISPs keep data for a short period of time afterwards, so it is still available.

Stuart C McDonald: What sorts of periods of time are we talking about?

William E Binney: I think that for most of them the figure with regard to their records is up to six months.

Stuart C McDonald: But do they do that? Is it a matter of practice?

William E Binney: Yes. On the web there is a list of companies' policies showing which ones keep data and for how long.

Stuart C McDonald: But at the end of the day you are accepting that there would be some practical utility in requiring the retention of records for six months.

William E Binney: Going after it in a targeted way, yes.

Stuart C McDonald: What do you mean by a targeted way, then?

William E Binney: Because you have at least the device that the person was using to connect with the internet, along with their phones and cell phones, so you have that data. You can use that data to go after them and data that was related to them.

Stuart C McDonald: Sure, but you would have to have retained en masse, because obviously you never know who is going to go missing, and then you have to go back.

William E Binney: The telephone companies keep that data for a period of time also, so you have that from them. You also have it from the ISPs for a period of time.

Stuart C McDonald: Okay. To both of you: what about the privacy implications of keeping internet connection records in the way proposed by the Bill?

William E Binney: To me, right upfront it destroys privacy. To return to the bulk issue, taking so much of it in destroys your capacity and makes your analysts dysfunctional. It

makes your law enforcement people dysfunctional, too. They cannot find the data that is important.

Jesper Lund: In terms of privacy, you would basically be storing the entire internet activity of every British citizen, which is really intrusive. In the specific case of finding a missing person, what would be most effective would be if their mobile phone was still active; then the mobile telephone company can triangulate that phone using its mobile phone towers. If the phone is no longer active, presumably that is where a case could possibly be made for accessing internet connection records. However, those records may show you internet communications but they are not able to distinguish between active communications and the background communications that would happen on a smartphone at any time, even if it was left alone in a different part of the country.

The Chairman: I remind the Committee that just before 4 pm I will have to call the Committee to order because of the vote in the Commons.

Q247 Mr David Hanson: Imagine for a moment that your objections are not listened to and there is a scheme in place under the Bill that operates as the Bill currently proposes. The Bill says that £247 million is available over a 10-year period for the running costs of the Bill. In your professional judgments, is that a feasible resource to meet the costs of the Bill as proposed?

Jesper Lund: If you want an ambitious system for collecting internet connection records, it will be more expensive than the Danish system. Extrapolating from the cost of the Danish system, taking into account the difference between the size of the UK and Denmark, the limited version that we implemented in Denmark would take up what is set aside for internet connection records, so I think it would be more expensive than £247 million.

William E Binney: I think that that might be a good estimate for the retention and storage of data. I am not sure that it would cover the cost of processing, interrogation and development of software to do all this and of managing the data once you have it, having analysts look at it, whether you need more analysts and so on. There are a whole set of costs that go with data acquisition.

Mr David Hanson: The costs are detailed in the Bill, but essentially the Government have currently allocated around £180 million for the costs of establishing the collection of bulk data. Is that reasonable for 70 million people over 10 years?

William E Binney: From my perspective, that should be reasonable.

Q248 Mr David Hanson: One final question. We have talked a lot about privacy. TripAdvisor, Facebook, Twitter, Hotels.com, Tesco, the Co-op and Spotify probably know as much about me as the Government do. Is that a problem, or is it just the Government you have a problem with?

William E Binney: I would say that all those companies cannot come and arrest you, charge you with crimes or retroactively do research on you. For example, if you take a position that the Government are not in favour of, you can become a target, as numbers of people have.

Mr David Hanson: I suppose my question is: is the bulk collection of data by all those private sector companies more or less objectionable than the bulk collection of data by the Government to stop terrorism, paedophilia, criminal activity, drug abuse and all the other activities? That is a conjectural point.

Jesper Lund: I understand the question. It is also one that has occurred to me several times in Denmark. The important difference is that you give consent to those companies to collect your data. You choose whether to use Facebook and you can refrain from using it if you do not have faith in its data collection practices. You cannot get out of internet collection records. They show your internet activity and they are going to be retained, whether you want that or not. As I understand the British system, not all communication service providers will sign up to this, but you will never know whether the information is retained—

Mr David Hanson: I suppose that that also presumes that I am bothered about that. If I am not committing a crime, am I bothered about the fact that they could access it if I did? I just pose that as a question.

Jesper Lund: Sure, but my take on this is that privacy is a fundamental right that applies to the individual citizen, just like freedom of expression. Whether or not you want to use that right is your choice, but the mandatory collection of something like internet connection records infringes your right to privacy.

Q249 Dr Andrew Murrison: It has been said that the UK intrudes upon the privacy of its citizens in a way that practically no other western state does. I am concerned that the UK should be an outlier, if that is true. Clearly the point of safety is being with the pack; indeed, in a legal sense it is probably important that it is. What is your assessment of where this Bill would place us in terms of countries with which we can reasonably be compared in terms of the acquisition of data and the surveillance and control of that acquisition by the state? Sorry, that is a very broad and overarching question, and this is a very complicated Bill and there are parts of it that will apply to a greater or lesser extent in other countries. As a broad-brush approach, though, where do you think it would place us?

William E Binney: I think it would place you equally with the US, because this is exactly what the US does. It does it under Executive Order 12333, which has no oversight whatsoever in the US.

Dr Andrew Murrison: No oversight at all?

William E Binney: None at all, by courts, Congress or anyone. It is all done by presidential order. The Fairview programme is the primary programme for the collection of data against US citizens, and it has 100 tap points right across the US, distributed with the population. It is distributed in that way because it gives them the ability to capture all that data about US citizens. That is a violation of our constitutional rights and we have been trying to challenge it in court. They have been fighting like blazes to keep this out of the courts because they know that what they are doing is unconstitutional.

Dr Andrew Murrison: Presumably, that is a work in progress.

Jesper Lund: It is always hard to do these comparisons, even within Europe because sometimes the European Union has similar laws. My understanding is that the UK is at the forefront of data collection about its citizens in Europe. France is also stepping up the surveillance of its citizens but is taking different routes in certain areas—for instance, by forcing communication service providers to do some form of metadata analysis of the communications that are going through their systems, not just the retention of those communications. You see different approaches in Europe but my short answer would be that the UK is at the forefront of data collection.

Dr Andrew Murrison: In terms of intrusiveness?

Jesper Lund: In terms of intrusive data collection, yes.

Dr Andrew Murrison: And what about oversight?

Jesper Lund: It is probably even more difficult to do cross-country comparisons of oversight. If I compare the UK and Denmark, I would say that you have more oversight in the UK but also more data collection.

The Chairman: It has been a fascinating session for all of us. Thank you both so much for coming along and answering a diverse range of questions, and a double thanks for travelling from abroad.

Witness: **Sir Bruce Robertson**, New Zealand Commissioner of Security Warrants (via video link)

Q250 The Chairman: Good evening, Sir Bruce.

Sir Bruce Robertson: Good evening.

The Chairman: Are we all here? This is the first time I have conducted a meeting with someone who is more than 10,000 miles away but we are very grateful to you, not least because of the unearthly time it is in New Zealand. Our deepest thanks to you. As you know, this is a huge Bill that Parliament here in the United Kingdom is going through. We have been set up to look at the Bill for pre-legislative scrutiny. We are composed of Members of the House of Lords and the House of Commons. We are particularly interested in talking to you about your experiences, and I repeat that we are very grateful indeed that we have this chance to do so.

I will open with a general question which will give you the chance, if you wish, to make some opening statements that you think might be useful to the Committee. Obviously we are looking at the comparative roles of the Investigatory Powers Commission and yourself. How does the role of our proposed new Investigatory Powers Commission compare to the job that you have been doing?

Sir Bruce Robertson: I think the fundamental difference between what is proposed and the task that I undertake is that my role is restricted entirely to the issue of granting the

warrant in the first place. I have no supervisory or auditing role beyond that point. We have a split between the power to allow an interception warrant to be granted and the supervision of what continues thereafter. When there is a desire on the part of either the security service or the GCSB to get authorisation, they make an application to the relevant Minister but the Act provides that the relevant Minister can grant an authorisation only if I concur with the granting of it. It is an entirely dual operation. From my experience of three years and the experience of my predecessor, who was in office for almost 14 years, this appears to provide a sensible and operational joint protective measure. Parliament has made clear the basis on which authorisation can be granted. Procedures and protocols are in place which ensure that this is done only when it is necessary, reasonable and proportionate and where there are no alternatives available.

When, as a judge, I was involved in the issuing of warrants to police officers—as a High Court judge my involvement was restricted to drug cases and criminal conspiracy—the issue was entirely about law enforcement. There was no executive involvement or activity at all. In the area of national security, there are, of course, two sets of issues that need consideration. One is whether what is sought is lawful. The second, which is the Executive's decision, is whether or not it is an appropriate course of action to be adopted.

I have the time, and I take the time, to investigate a proposal or a request in some considerable detail. As I said in some of the earlier material I submitted, when there is an application I receive an indication that this is afoot and I go to the premises and first of all read the file. The file, as is inevitable in this sort of area, will be voluminous but I have the time to do that. I have the time to analyse it. I have the time to dissect it. What is as important as anything is that I have the opportunity to actually meet the people involved with the application. When the formal steps are taken, the director will be there, but at the earlier stage I meet the people, first, in the legal division and, secondly, those who are moving on the ground, to discuss what is sought and why it is necessary, why it is proportionate and what is available. It is not uncommon for there to be some tweaking or tightening at that less formal stage. Then I meet the Minister in person to discuss our joint responsibilities in respect of that issue.

It is important, however, that once that has been done and a warrant has been granted and issued, I am not involved in the auditing process of whether it has been properly put into effect and the operations are appropriate. That is part of the remit of the Inspector-General of Security and Intelligence. She has a substantial staff. I do not have a staff; we are dealing with a relatively small country. Of course, the difference between our situation and yours is that my involvement is entirely in the security area. I do not have any involvement in other areas of law enforcement.

The Chairman: Thank you very much. Can I ask you about the very urgent cases that from time to time come up? In the system that you have just described, how do you operate when an extremely urgent case appears before you?

Sir Bruce Robertson: I put on my running shoes and I get myself to the Minister's office. There is inevitably a period of some hours. In the cases that are truly urgent and need something done in a great hurry, I will be contacted at the time that they are trying to set up an application time with the Minister. Sometimes the reading and briefing that I do will be truncated and might occur in a foyer or in the lobby of the Minister's office. I have been pulled out of dinner. I have been pulled out of my bed. But it is not a frequent thing,

at least in New Zealand. In the overwhelming number of cases, the two services operate on the basis of having a little time. It is not impossible to get a retired person, when they are required, to be available as quickly as the Minister would need.

The Chairman: Thank you very much. That is very clear.

Q251 Mr David Hanson: Good afternoon. You mentioned in your submission that your predecessor held the post for 14 years. The proposal in the Bill is for the position to be held on a three-year contract. Do you see any advantages or disadvantages in that length of appointment?

Sir Bruce Robertson: Sorry, I was perhaps less clear than I should have been. The appointment is for three years, but my predecessor was reappointed on a number of occasions. My appointment is for three years, but I can be reappointed. It makes a lot of sense to have an opportunity to reassess because one has the normal powers and protections that a judge would have. Removal is by grace of Parliament. Under our system in which the appointment is made by the Governor-General on the advice on the Prime Minister after consultation with the Leader of the Opposition, it is sensible that there should be an opportunity for periodic review.

Mr David Hanson: The method of appointment proposed in the Bill in the United Kingdom does not involve the Opposition and is a prime ministerial appointment in consultation with the devolved Administrations in Scotland and Northern Ireland. Do you think that the New Zealand model with a Governor-General appointment on recommendation with consultation with the Leader of the Opposition is just different or is it better or potentially worse than the current proposal?

Sir Bruce Robertson: It seems to me that there is a strong argument for the most independent position that can be created to be created. That is done in New Zealand by appointment by the Governor-General. Because of the sensitivity of this area and the importance of public confidence in what is done, the requirement to consult the Opposition before the recommendation is made is worthwhile. Much of this is about the perception of whether there is an independent, objective inquiry going on by a person who is clearly independent of the Government of the day. My predecessor was obviously appointed by different Governments of different hues over the years. He was simply seen as a person of enormous integrity who had the ability to do the job. It was in no way a "political appointment".

Q252 Lord Hart of Chilton: Good evening. As you have been a judge for more than 18 years, independence runs through you as a sort of DNA characteristic.

Sir Bruce Robertson: I hope so.

Lord Hart of Chilton: How do you maintain that independence from Ministers? Does that mean that you foreswear all cocktail parties and all dinners and do not go to rugby internationals where they might be? How do you go about it?

Sir Bruce Robertson: None of the matters that you have alluded to would have interfered with my independence in the task I was carrying out. In the 28 years I was a judge, I had no difficulty in reaching a view different from that held by the Government or any other

litigant with whom I was involved. My task now I see as simply analysing and assisting with the evidence. The great attribute which an experienced judge ought to bring to the task is the ability to weigh and assess and sometimes to put a fairly weary eye across a proposal. I do not think any of us should ignore the fact that in this area of public life, as in others, there will be very committed views which are genuinely held which do not always stand up to the strictest scrutiny. In speaking with quite senior officers who, let us say, have reached a view that there is no alternative to what they propose, they can be challenged, questioned and the like. When it comes to the Minister, when I was appointed to the position in New Zealand the relevant Minister was the Prime Minister and I was not overawed by that in any way, nor am I overawed by the fact that the Minister at the moment is the Attorney-General and Minister for Security. Both the people I have dealt with have been capable of fairly rigorous debate with me. As a judge obviously you have to maintain, for public confidence, a degree of independence, but that is the way it is in the life of a judge, so there is really nothing different about that.

Lord Hart of Chilton: Thank you. Does the draft Bill include sufficient safeguards to uphold this important dimension of the independence of the commissioner's role?

Sir Bruce Robertson: As a matter of policy, the ability to be independent, objective and effective is enhanced and embraced if the input is prior to the issuing of the warrant. As I perceive what is proposed under your draft Bill, a person in my position would come in after the event. That becomes a matter about the standard of review and the manner in which that review occurs. It is a much more powerful, potent and effective check if the person in my role is involved in the initial granting of the warrant before anything is being challenged.

No matter what words you put around it, as soon as you get a challenge to something which has already occurred, all sorts of questions arise about whether it was a permissible activity and whether it should be altered. That is the issue in judicial review in the normal court system. The New Zealand arrangement allows independent involvement before the warrant is granted so that the question of whether what is proposed is lawful in its widest sense is part of the initial assessment, not an after-the-event review. There is real advantage in what we do.

Lord Hart of Chilton: Does that mean that you, in considering and reviewing before the event, are able to substitute your opinion for that of the Minister?

Sir Bruce Robertson: The Act says that we each must agree about what can occur. As a matter of common sense and the separation of power, it would not be for me to become involved in issues of high policy providing they are matters which are legally able to be undertaken. So although the Act does not categorise the area in which each of us works, it is inevitable that we bring different skills, experience and assessment to the task. In New Zealand, our Parliament decided that these two matters were of equal importance and that both should be given proper scope and operation before the warrant is granted. If what was being asked for was lawful and proper in the terms that I have talked about previously, then it would seem to me a very unusual situation if I were to endeavour to force my view on an issue of high policy on someone else. But let me say that it is not a matter that has created issues. I have at times raised with a Minister my concerns about a proposal. We

have been able to talk it through and have reached a common view, but that is not a commonplace problem.

Q253 Lord Strasburger: Good morning, Sir Bruce. Still on the subject of independence, how is your budget and the budgets of other intelligence oversight bodies in New Zealand set? Are they set independently of the Government?

Sir Bruce Robertson: They go before a Select Committee of Parliament which has responsibility, and a local budget is granted to them. It is not a matter in which I have any particular involvement because my activity is restricted to a relatively narrow area, which, at least in my judgment, requires my personal involvement and intervention. I have no need for a budget of any consequence or size for myself. The issue of how the Secretary-General, who does have a large staff, operates is a quite separate one on which I shall not comment.

Q254 Suella Fernandes: Good morning. I would like to look a little more at the comparison between ministerial authorisation and judicial authorisation of the warrants. As you know, in this country it has traditionally been the Home Secretary or Ministers who have the power to issue these, in contrast to the situation you are setting out. To be clear, when you are considering your decision, you apply a legal test. That is right, is it not?

Sir Bruce Robertson: The Act does not restrict in that way. I am saying that it is a matter of operational activity. That is the real strength which I bring to the activity. In ensuring this careful check and balance, it does not appear to be part of my role to intrude into other areas to the extent that what is proposed is lawful and therefore available, but perhaps in my personal view not as prudent as it might be. I would not hesitate to express a view or to question a matter, but I am doubtful that in that narrow area I would be likely to want to force my view on another. It is difficult for me to see how that would be appropriate, but my experience is that that is not a decision I have ever been forced to take.

Suella Fernandes: So you apply a narrower legal test that is more limited in scope—would you not agree?—than a potential political approach, which would include factors such as high policy, as you describe it, or a sense of the national security issues, the nature of the threat, or even the additional factors of diplomatic or reputational risks to the issue of a warrant. They are not necessarily relevant factors in your decision-making process, are they?

Sir Bruce Robertson: The Act does not say that I am excluded from consideration in that area. The Act says that together we will grant a warrant and make an authorisation. I am simply saying that, as a matter of practical reality, in my assessment of diplomatic repercussions, high policy and that sort of thing, I would not seek to hold the line in the way that I would with regard to whether a measure was actually lawful. The question of how a person exercises authority is partly a question of serious judgment. There are competing interests which have to be dealt with. Provided that the alternatives are lawful, I do not see that it is my task to impose my personal assessment of a situation. But, as I say, I do not see why, as part of the overall process, I should not be involved in questioning or challenging to ensure that the requirement of legality is still being met.

Suella Fernandes: One last question. In terms of your decision-making, in the event of a mistake or some other error, what is the accountability that you have to meet? What is the appeal route and the scrutiny that you are held to?

Sir Bruce Robertson: The Inspector General, as part of her general remit, can look at issues around the granting of a warrant and can report on that, but my position is not one in which I am held out publicly to be questioned or assessed. This is the general process of auditing and supervising, and we are part of that process, but there is not an individual way in which the commissioner, any more than the Minister, is called to stand up in the marketplace and explain what they did and why they did it.

Suella Fernandes: Although would you agree that, unlike a Minister, your role is less public—or, to put it another way, Ministers are elected and more public-facing, and therefore have an element of greater accountability?

Sir Bruce Robertson: In all my years as a judge, although I could not be called to account in the way that you are speaking of, I did not ever think that I was not accountable publicly. Certainly in the environment in which we live now, in your country and mine, judges are the subject of discussion by the public in a very general way, and no doubt could be in this situation. However, I accept that I am not held out in a way that a Minister can be because they are elected.

Q255 The Chairman: You have explained very clearly, Sir Bruce, that in your decision-making on this matter you concentrate on the legality, but that you are not restricted by legislation so to do. Would you occasionally take into account proportionality and necessity as well as legality?

Sir Bruce Robertson: Proportionality and necessity are part of legality. As I see it, the regime in my country and that proposed in yours require that proportionality, alternatives and reasonableness are all matters that go to the legality of what is proposed. That is why I do not see a hard line between the one and the other, and why it would not be practical to say that a person in my role is entitled to have a legal involvement. The two are inevitably intertwined. I am saying simply that when it comes down to a question of national security or high policy, my personal assessment should not be given undue or particular weight if the alternative proposed is otherwise a lawful alternative that is available.

The Chairman: Thank you very much. That is very clear.

Q256 Dr Andrew Murrison: Good morning, Sir Bruce. You paint a picture in New Zealand of a fairly collegiate approach to warrantry on national security matters. I suspect that that would not wash terribly well here, and certainly the draft Bill before us at the moment is not drafted in those terms. Indeed, it is quite specific: the judicial commissioner who is proposed here would be bound by the general rules of judicial review. What do you think about that? Do you think that a merits-based assessment by the judicial commissioner of the sort that you are describing would be more appropriate? Would you comment on what happens in New Zealand in the event that the collegiate approach that you have described breaks down and you disagree with the Minister or some subsequent Minister, or your successor disagrees with subsequent Ministers? Bluntly put, who wins, or is it a default position that the application fails?

Sir Bruce Robertson: My involvement at the stage at which I am involved is a much more potent force for providing protection for the general public. I have to say that in my term a total impasse has never arisen; we have been able to come to an accommodation and an

agreement that was acceptable to both of us. Technically, the position is that if a commissioner were unable to agree to a course of action, a warrant could not be issued. There is no doubt about that. The position, which you describe as collegiate, I see simply as one in which two people, each with experience and total integrity, reach a view on the available evidence. One of the important values that I can bring to the task is that there must be an evidential basis rather than a hunch or an emotive reaction of some sort. There needs to be some material that can be pointed to which justifies this degree of state intervention. When you come to look at the subsequent scrutiny by a judicial officer, it is inevitable that the paraphernalia around judicial review will emerge. That is a less potent force than when you have early involvement prior to the granting of the authorisation. What we are talking about is balancing competing interests, including the interests of people who cannot and will not know that the process is going on at all. What you decide is the extent to which you want to have a rigorous legal assessment before there is any authorisation. The subsequent activity, and the supervision and auditing that goes on, does not provide the same heightened level of protection that the New Zealand model can.

Q257 Stuart C McDonald: Sir Bruce, you have already pointed out that you have no supervisory or auditing role. That is very much in contrast to what is proposed in the Bill. Would the Bill be improved by including a similar split to the one in New Zealand?

Sir Bruce Robertson: The most that I could say is that the New Zealand system works. It enables an early involvement of the claim of legality. I would be uncomfortable about a position in which I was required to second-guess and reassess what I had already agreed to at an earlier stage. The division appears to me to be workable and to be strong in its principled approach.

Stuart C McDonald: That is very diplomatically put, thank you.

Sir Bruce Robertson: I do not know that I have a reputation for being diplomatic.

Q258 Matt Warman: To pick up on an earlier question, are there any circumstances to your knowledge where the time that it has taken you to get together with the Minister and have the conversation has held up the operational effectiveness that the security services might like?

Sir Bruce Robertson: Not to my knowledge. I suspect that sometimes the relevant people probably find it quicker and easier to keep me available in a spot than they do the Minister. I have been pulled out of a dinner and out of my bed, but I can operate less quickly and have fewer ongoing demands on my time than the senior Minister would have.

The Chairman: Sir Bruce, we are indebted to you for a very valuable session. The international comparison has been intriguing. Again, our apologies to you for it being so early in New Zealand, but this has been very important for our Committee's deliberations. Thank you.

Sir Bruce Robertson: Thank you so much. Good morning.