HOUSES OF PARLIAMENT

Joint Committee on the Draft Investigatory Powers Bill

Oral evidence: Draft Investigatory Powers Bill, HC 651

Wednesday 13 January 2016

Watch the meeting

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

Questions 259-282

Witness: **Rt Hon Theresa May MP**, Home Secretary, gave evidence.

Q259 The Chairman: A very warm welcome to you, Home Secretary, for agreeing to give evidence to the Joint Committee this afternoon. You are between the 20th or 25th, I think, of the number of evidence sessions we have had, and, indeed, the last. It has been a fascinating couple of months talking to people from all walks of life, with different views on this subject, but we particularly welcome you, for obvious reasons. It is your Bill, it is one of the biggest Bills that Parliament has ever seen and it is extremely important. We live in dangerous times but we live in times in which it is so important to protect our liberty as well. It is that balance between security and liberty that the Committee is looking at in great detail. So welcome to you.

I am going to start by asking you a question, but if, after I have asked the question, you want to say a few words by way of introduction, the Committee will be more than willing to listen to that. My question is one on process as much as anything else in that the Information Commissioner and the Interception of Communications Commissioner, among others, have suggested that the Bill should be subject to a sunset clause, and if not a sunset clause for the whole Bill, possibly for parts of the Bill. What are your views on that?

> ***Theresa May MP***: Thank you very much, Chairman, and may I take this opportunity of thanking the Joint Committee for the work that you have been doing? I recognise from the number of evidence sessions you say you have taken that it has been a very thorough piece of work that this Committee has been doing on, as you say, what is a significant Bill, both in size and in the powers that it holds within it, significant also because of the nature of the threat that we face and the necessity of ensuring that our agencies and police have the powers that they need to keep us safe—with, of course, appropriate safeguards.

In a sense, it is against that background that I would say that from time to time Parliament does put sunset clauses in legislation, often particularly where legislation has been put through perhaps in an emergency. A recent example in this area was DRIPA—the Data Retention and Investigatory Powers Act—which was put through fairly quickly largely in response to a decision in the European Court. It had a sunset clause enabling us to put into place a longer-term process of developing a piece of legislation that would stand the test of time. That would be my concern about attempting to put a sunset clause in this. We have tried to balance here the need, in a sense, to future-proof the legislation against the need not to produce something so wide-ranging that people feel it is not clear on the powers that are going to be used. RIPA has been in place for 15 years. We would anticipate or expect that this Bill would stand the test of time.

The other aspect to it is that there are certain parts of the Bill that require companies—communication service providers—to take certain actions. Sometimes those actions are ones that require careful planning, and, if you put sunset clauses in, it gives a degree of uncertainty to those very people whom government might be requiring to take certain actions to keep us safe.

The Chairman: A point that has been made, as opposed, for example, to the Prevention of Terrorism Act, which had to be renewed every so often because of the nature of the legislation, is that this Bill is different in the sense that it attempts—and successfully, I suppose—to bring legislation up to date with regard to advancing technology. Would it not be the case, though—and it is inevitable, I suppose—that technology is going to advance even more and that from time to time Parliament would have to have a look at its legislation to deal with that advance in technology?

Theresa May MP: Yes. I am certainly not trying to give the impression that I think this is a Bill that will last for ever and a day. As technology advances, it may be necessary to revisit the powers, the legislative framework and the safeguards that are available, but I do not think advances in technology are going to move according to sunset clauses established by Parliament. The necessity that may come in due course to look again at aspects of the Bill, should it become an Act, would have to be dealt with as and when that arose, rather than artificially putting some deadlines in that might not meet the requirements in relation to the advances in technology.

Dr Andrew Murrison: Home Secretary, do you recognise that there are significant areas of uncertainty in the draft Bill presented to us for consideration at this stage and that some of that uncertainty may very well need to be resolved at a future date? That would mean, naturally, that a sunset clause or a defined period over which this Bill would be in force for review at some future date, perhaps even on a Parliament-by-Parliament basis, might help to deal with issues such as resolution of IP addresses and the definition of ICRs, which remain unclear despite an attempt by the Home Office to improve the definition of ICRs. We sense that, even now, those definitions are unclear—and will be unclear to CSPs especially—and will need to be revisited at some point. In the Bill, if we were able to have some certainty over what sort of period we would be able to do such a thing, it might make for better legislation going forward.

Theresa May MP: I am afraid, Dr Murrison, that I am not sure I recognise completely the impression you have given of the Bill in terms of the degrees of uncertainty that rest

within it. You are right that we have introduced a greater degree of clarity in relation to the definition of internet connection records. On the IP resolution, of course, we did pass legislation in the Counter-Terrorism and Security Act in relation to that. The ICRs provide the final piece of that picture, if you like, in being able to identify people. There are cases today, for example, in paedophile networks, where that identification is not possible because we do not have the ICRs.

There is still a degree to which sometimes people are looking at this and thinking about what was in the draft Communications Data Bill, which was not progressed with by the previous Government, and perhaps transposing that into this Bill. We have tried to be very clear on what ICRs are and, indeed, have limited the use of ICRs within this legislation. I know law enforcement has argued perhaps for a wider use of them, but we are proposing that the balance is best met by limiting those within the Bill. With regard to CSPs, we have not had, as far as I am aware, indications from them that in any sense they do not understand what we are talking about in looking at ICRs. We have had numerous meetings with communication service providers as we have been going through the process of determining what should be in the Bill—and the discussions are ongoing—about the technical aspects of the Bill and have had reassurance from the CSPs.

Dr Andrew Murrison: Could you give the Committee your definition of an ICR in terms that might be understandable by a lay person?

Theresa May MP: I will try to do it in an equivalence way in the sense that, when you have somebody who is accessing a particular site or is using the internet for a particular communication, you wish to be able to identify that. You are not trying to find out whether they have looked at certain pages of a website, which is where I think the confusion may arise because of what people felt was in the draft Communications Data Bill. It is simply about that access to a particular site or the use of the internet for a communication.

Q260 Mr David Hanson: We have had some compelling evidence about the need for the Bill in relation to the prevention of terrorism, crime and drug abuse and in tracing missing persons from the policing agencies—compelling evidence—but there still remains a body of opinion that worries about the privacy elements of the Bill and what security their own privacy can be given by the state in relation to the access to that information. I think it is really important that you set on the record now for the Committee and the general public what steps you believe need to be taken to retain and secure that privacy, and what associated steps can be taken to minimise risks for the loss of that privacy.

Theresa May MP: If I may, there are three aspects that I would talk about in relation to privacy. You are right, Mr Hanson, to set it out. One of the meetings I had was with representatives of various victims' groups—victims of sexual violence, for example—who were very clear, along with law enforcement, of the importance of the powers in the Bill. The safeguards available for individuals in relation to the powers within the Bill are various. First, there are the authorisation procedures, and in relation to the most intrusive powers, namely interception, we are enhancing the authorisation procedure by introducing the double lock of having the Judicial Commissioner looking at a warrant as well as the Secretary of State. There are also the oversight provisions that are provided at various levels, also by the new Investigatory Powers Commissioner—currently provided by a number of commissioners but, as you will know, to be consolidated in that office—who is

looking to make sure that the agencies are using their authorities in the correct way and that proper processes are being followed. There is the oversight that is provided by Parliament itself through the Intelligence and Security Committee. So there are safeguards in authorisation and in oversight.

Then there are also requirements where data is being retained by companies. There are various requirements in relation to the various Acts that those companies need to abide by, such as the Data Protection Act and the Privacy and Electronic Communications Regulations 2003, which require data to be held by the companies in a secure fashion—so, securely. Of course, we introduce the offence in relation to misuse of data that is being retained by the companies.

Q261 Mr David Hanson: There remains a concern as well, though, that communications data definitions—and Dr Murrison has touched on this—remain relatively vague. For example, Clause 195(1) says, "data includes any information which is not data". What does that mean?

Theresa May MP: I completely understand people raising an eyebrow or two at that particular sentence, which I did when I read it myself. I am happy to look at the wording, but it is an attempt to do something very simple. If you talk about data, a lot of people tend to think only about computer stuff—electronic records. We are saying that when we use the term "data" in the Bill it can cover, for example, paper records as well. It is an attempt to be helpful, which, in its language, it has not been.

Mr David Hanson: In an attempt to be helpful—and I genuinely want to be helpful on this occasion—would it be sensible even for the Home Office perhaps to look at the idea of a prescribed list of the elements that comprise communications data and publish them in a statutory code? Would it be helpful to look at separate definitions of entities and entries for telephone data and internet data? I simply ask that because the type of reassurance that that could give might well help the passage of what, as I said at the start of my contribution, is a compelling case for the Act as it will be.

Theresa May MP: Yes, and I completely understand the aim of your question and the intent behind what you are suggesting. The problem is—and it goes back, in a sense, to the first set of questions that I had and the point that the Chairman himself raised—that we are trying to draft legislation that will operate in what can be quite a fast-moving technological world, where things are developing. The more you try and prescribe in more and more specific definitions, the harder it becomes and the shorter the life of the legislation is likely to be. That is a point that David Anderson has made in relation to this. As I said earlier, it is a balance between trying to ensure that legislation is so drafted that it is clear for people but that it is not so drafted that it means it will only have a very limited life, precisely because definitions will move on and there will be developments.

Mr David Hanson: The fast-moving nature of change is one of the potential worries as well. On a personal basis, I did not use Twitter five years ago; I am using it now. I did not have Facebook three years ago; I have it now. With the changes in life—I do not know what is going to come next—I wonder whether or not, going back to Dr Murrison's point again, the definitions are such that they are full of clarity for now and for the future.

Theresa May MP: That is precisely why we are trying to be technology-neutral in the sort of language that we use within the legislation, precisely so that we can provide for developments that may take place in the future. You raised the issue about entities and events. "Entity" is an individual, a device, an event or a communication between devices, for example. The more you try and list, "by definition, communication only covers these issues", then you have, automatically, potentially limited—

Mr David Hanson: But there is a sort of halfway house between a sunset clause on the Bill and a statutory code that could be issued potentially every two years indicating what is covered by the Bill. Would that be a feasible and possible thing to do to offer the security to those who still have the concerns that I expressed earlier?

Theresa May MP: The only comment I would make—and I hope it follows on from what I have been saying—is that if you have a period of time for which a particular code is in operation, unless you have some very easy ways of changing that, you are going to be bound by it for that period. If something comes up in between, you may find that you are caught unable to use a power in a way that is necessary to keep people safe because of the well-intentioned attempt to try and give greater definition in these matters.

Q262 Suella Fernandes: In relation to communications data we have heard evidence from the head of the Metropolitan Police Service Technical Unit, who has said on record that they are struggling to keep apace with technological development, and the use of communications data is integral, in theory, to inquiries into theft, child sexual exploitation, homicide and fraud. What is your opinion on extending the number of purposes for which law enforcement and agencies can obtain communications data—for example, for the purpose of saving life, such as identifying vulnerable individuals in circumstances that may not be considered an emergency?

Theresa May MP: It is important that access to communications data is available in circumstances where it is about saving life. The definition of an emergency will cover a whole range of circumstances where the police will suspect that somebody is in danger and that there is a requirement for them to access this data. That is why I have been comfortable with using that phrase in terms of the emergency. I have tested with my officials certain circumstances where saving a life might arise, and I think in all those that I have looked at it would be covered by the definition of emergency. Almost by definition, if the police or another authority are trying to intervene to save a life, that is an emergency circumstance.

Suella Fernandes: The case that comes to mind is that of a missing person where there is a suspicion or information that someone has gone missing and they are a vulnerable person, but in the current regime there is a difficulty in defining that necessarily as an emergency.

Theresa May MP: There are a lot of developments taking place in how police deal with MISPERS—missing person cases—but if there is a suspicion and a concern that there is a genuine threat to life for that individual, I would expect that to be able to be covered by the use of the term "emergency".

Suella Fernandes: What is your view on extending the purposes to cover those crimes that are not "serious crimes" but where it is still necessary and proportionate to obtain that data?

Theresa May MP: It is important for law enforcement to be able to access communications data in these circumstances. There is a formal definition of serious crime, but there will be other crimes—for example, maybe harassment online—where access to data is important to identify perpetrators and deal with that crime but which does not necessarily fall into the formal definition of a serious crime. It is for that reason that it is important for the police to be able to have access to communications data in other circumstances.

Q263 Shabana Mahmood: Home Secretary, could I take you back to the issue about internet connection records and the definition, following on from your exchange with my colleague Dr Murrison? We have only recently had the Home Office's submission with the additional information. We have not had an opportunity to put that to all the numerous witnesses who have given evidence or might have wanted to give us written evidence on those. Our very preliminary advice or initial soundings are that the issue is not that there is no understanding about where you are trying to get to. In fact, you said in your answer that there is understanding of what you are talking about and your dream scenario of the information you are trying to get to. The problem is whether it is technically feasible, given the way that the internet works. Our understanding at the moment is that there is no real agreement or understanding of the technical path to get you to the kind of data that you want. What is it that makes you so confident in the answer you gave earlier that that technical path to your best scenario for internet connection records is going to be found and met by all the CSPs?

Theresa May MP: The confidence we have comes from the discussions that we have been having with CSPs. As I indicated earlier, we have had numerous discussions with them about how access to ICRs may be achieved. Chairman, in my answer earlier to Mr Hanson and to Dr Murrison, I was not trying to suggest that there would be no way in which we would be trying to get some greater clarity of definition perhaps through codes of practice. There was a specific issue around timetabling and so forth. We are talking to the CSPs, and the discussions we have had with them have been about some of these technical issues about access. There are different ways in which different providers approach the way they operate, but we are confident from those discussions that it will be technically feasible for us to ensure that there is access to the information that is necessary.

Shabana Mahmood: Even if each of them goes about it slightly differently, you are confident that the end product will be basically the same.

Theresa May MP: Yes; we are confident that we will be able to have the access that is necessary.

Q264 Shabana Mahmood: A lot of my constituents wrote to me about this description of internet connection records being like an itemised telephone phone bill. Other people have said—and lots of Members of Parliament can relate to the sorts of communications we have had from our constituents—that this is a very unhelpful, misleading characterisation of what an internet connection record will look like. Would you agree that that is probably not helpful and we should avoid it?

Theresa May MP: It is, again, another attempt to be helpful in describing. The point of the comparison is to say that at the moment law enforcement and agencies have access to data in relation to telephony, which enables them to identify, if somebody has gone missing, with whom they have been in contact prior to going missing. As people move from

telephony to communications on the internet, the use of apps and so forth, it is necessary to take that forward to be able to access similar information in relation to the use of the internet. I would say it is not inaccurate and it was a genuine attempt to try to draw out for people a comparison as to what was available to the law enforcement agencies now—why there is now a problem—because people communicate in different ways, and how that will be dealt with in the future. It is about communications from one device to another.

Q265 Shabana Mahmood: I suppose in a way your answer helpfully illustrates the difficulties that we are all grappling with when it comes to how to accurately describe exactly what is going on.

Can I move on to the experience of Denmark? We have had a fair amount of evidence on how a similar regime worked in Denmark, which was then ultimately scrapped. There were some very significant differences between what happened in Denmark and what you are proposing here, in particular the coverage of the scheme, as it were, in Denmark; their scheme did not cover access to the internet by smartphones for various technical reasons, but there were similarities around the desire to have IP address resolution and so on. They found in Denmark that they just collected a huge amount of data of limited utility. It was not particularly effective in helping the police to do their job. What is your view of what happened in Denmark, and why would you say that what you are proposing here is significantly different and therefore more likely to be useful?

Theresa May MP: As you might imagine, we have been talking to the Danes about their experience. There are a number of ways in which it is different. One of them is in relation to how information is due to be collected. I would best describe it—as it was described to me—that part of this is about at what point on the network you are accessing the information. We will be accessing it at a different point from the point at which the Danes were accessing it. They were getting a lot of peripheral information that did not enable them to link accounts to users, as I understand it. Another element is what we have already done in relation to IP address resolution through the Counter-Terrorism and Security Act. When you put these together, it gives us that greater capability.

There are some other differences in relation to costs, for example, in the Danish system. As I understand it, the costs were borne largely by the CSPs. We have an arrangement for providing for cost recovery here in the UK. There are a number of differences, but, in talking about the point at the network, it is trying to do it in a simplified way, which shows that there is a technical difference in the way we are doing it.

Shabana Mahmood: I understand the technical point you are making. One thing we have had quite a bit of evidence on is the amount of data you will be collecting and what it will ultimately tell you. One of the problems we have had some evidence on is about constant connection and that smartphones will almost always be connected to the internet by all the different apps. Therefore, the information you are collecting is only going to tell you the point at which the app was activated and not anything else because it is constantly connected to the internet. Do you see a danger that, in the end, you will just collect a vast amount of data that is of limited utility to the police, if, for example, in a missing persons case all they can tell is basically when somebody downloaded an app on their phone and not very much more than that?

Theresa May MP: Certainly in relation to this issue of volume of data, which was something that was raised in the Danish example, they did find that they had a large volume of data. We will have a more targeted approach, which we believe will reduce that overall volume of data recorded and reduce the risk that connections are missed. I was hesitating to say, Chairman, that I am reliably informed that the Danish implementation was based around sampling every 500th packet rather than recording individual internet connections or sessions, which is what we propose to do. I do not think there is going to be that volume of data in the much more targeted approach that we will take.

Q266 Stuart C McDonald: I have a couple of questions on internet connections, if I may, Home Secretary. Correct me if I am wrong—it has been a few weeks since I have read it—but the operational case for internet connection records is about 25 pages long. As far as I can see, it does not contain any mention of terrorism. Instead it focuses on fraud and child sexual exploitation. Is there a particular reason for there being no mention of terrorism in that operational case?

Theresa May MP: No. The case in relation to communications data and internet connection records has been one on which particularly the law enforcement agencies have given some examples of ways in which they can show the importance of this. That is one reason why we have tended to focus on that, and we can give those sorts of case examples in relation to that, but this is a capability that would be available to law enforcement and indeed to the agencies. I do not think there was a deliberate attempt to exclude terrorism, but, in looking at the operational case, sometimes it is easier to explain some of the cases that relate to issues like paedophiles and child exploitation.

Stuart C McDonald: Following on from what Ms Mahmood has been saying, there is one set of arguments about the utility of these internet connection records. For example, as you explained it earlier, an internet connection record would explain that I had contacted the Facebook website but it would not tell me who I had been communicating with or when and so on; so there are questions about the utility of that information. On the other hand, if you were to put together 12 months of my internet connection records, you would find out a hell of a lot about me, and I will not go into what you might find out about me. You can see why that would be quite invasive on the one hand and yet on the other hand there is this question about utility. How would you respond to those concerns?

Theresa May MP: As I indicated in response to an earlier question, the intention of this is not to find, in some sense, people's web-browsing history, which I think was one of the issues that was raised in communications data, looking at exactly what everybody was looking at all the time and the pages behind the first web page that they went to and so forth. As you will have seen in the legislation, we have limited the purposes for which access to internet connection records can be used. As I said earlier, law enforcement, I know, have indicated that they would prefer to see fewer limits. They think they can put a case for extending that. We have looked at the balance of the concerns that people have had about privacy against utility and that is why we have come up with that specifically limited set of access arrangements.

Stuart C McDonald: The response to that might be that, if you are going to start gathering this data and it is quite invasive, you might as well use it for a broader range of purposes. Going beyond that, you have recognised that the operational case concerns examples from

law enforcement, in particular, but we then get to the stage where it is a struggle to see why finding out that a missing person has been using Facebook cannot be done by other means—simply by speaking to the person's friends or family or by going on Facebook directly. Can we get more examples of the utility of these internet connection records that will help to persuade us that this invasiveness and collection of data will be worthwhile and worth the dangers that come with it?

> ***Theresa May MP***: I note the point that you made earlier about the potential arguments for increasing the purposes for which the information is collected. One of the benefits of the joint scrutiny committee is that it is a Committee that can challenge and look at those issues and make recommendations. If you are asking whether we can provide some extra examples and exemplifications that could show the utility of internet connection records, I am very happy to do that for the Committee. You mentioned a number of ways in which police would gain other information in relation to a missing person. Of course, in any investigation that the police undertake, whether it is for a missing person or whether it is a murder investigation, they look at a variety of forms of evidence in order to build the picture that they need to have to solve the crime or save the life. What they are saying—and what I am saying—is that as part of that, against the background of appropriate restrictions, oversight and safeguards, it is important that they are able to have access to this part of the picture as well.

Victoria Atkins: This follows on, Home Secretary, from Mr McDonald's question about the operational case, particularly with regard to terrorism. Yesterday Assistant Commissioner Mark Rowley, who leads the counterterrorism operation nationally, gave evidence to the Home Affairs Select Committee that communications data is used in 100% of terrorist investigations and prosecutions. Does that accord with your knowledge as Home Secretary?

> ***Theresa May MP***: Yes, it does. It is also my understanding that it is used in something like 95% of serious organised crime cases—often, evidentially in prosecution.

Victoria Atkins: So those percentages are very much in mind when considering the civil liberty arguments that many witnesses have given to this Committee.

> ***Theresa May MP***: Yes, indeed. I recognise that, because of the nature of the powers we are talking about in this Bill, it is always necessary to look at the utility argument and at the privacy argument. Communications data is an important part of the process that law enforcement, in particular, will go through when looking at these cases—when dealing with terrorist cases, as Assistant Commissioner Rowley has said, but in serious and organised crime cases as well. That is why we think that, in the internet age, we need to have this extension in relation to internet connection records. What is important—and what we are doing in this Bill—is the oversight arrangements. It is important that the legislative framework is right, the oversight arrangements are right and the authorities and safeguards are right, so that people can have confidence in the system, while knowing that, if this information was necessary in order to keep people safe, it would be available.

Q267 Mr David Hanson: I turn to data retention. The Bill proposes storing internet connection records for 12 months. I have three simple questions. How much will it cost, when will the capability be available, and who will pay?

Theresa May MP: We have provided some indicative figures in relation to—

Mr David Hanson: You have. It is £247 million in the Bill.

Theresa May MP: Yes. As I said, we have provided some indicative figures. Obviously we are still in discussion with individual CSPs about the ways in which these capabilities would be provided. We provide reasonable cost recovery. That has been a long-standing policy of the UK Government, where we are requiring companies to do things in order to have this sort of access.

Mr David Hanson: At one oral session on 14 December, we heard evidence from Vodafone, O2, EE and the regulatory engagement officer from 3. That is just four providers. Basically, they said that they alone could spend the £247 million and that they do not have the capacity currently to store the records required by the Home Office. The challenge to you from the Committee is, can you justify to us today—or at some point—that there is sufficient resource to meet the requirements that have been placed on providers and that they have the capacity to put this into practice in a reasonably short amount of time? Can you also indicate what the repayments will be? For example, Adrian Gorham of O2 said, "It is going to be huge". Mr Jonathan Grayling of EE said, "If there is a cost recovery model that places a cap on cost", it will be very difficult for them. These are important issues. Whatever our objectives, can you deliver it, for the budget that you have, in the timescale that you want, to the satisfaction of the providers?

Theresa May MP: Precisely one of the reasons why we are having such detailed discussions with providers is that we have been going through this and talking to them about the sorts of ways in which this would be provided, about the technical feasibility of it—that is why we are confident of it—and about the sums of money that would be necessary. If the Committee would like some further indications in relation to those matters of technical feasibility and cost, I would be happy to provide them. We have not just been sitting there as the Home Office saying, "We think this is a good idea. Let us pluck a figure out of thin air, put it into the Bill and the explanations, and just hope and pray, on a wing and a prayer, that people can do it". We are talking to them in detail about how this would be provided, and they have been responsive. I can say that, because I myself have had a number of meetings with CSPs at which they have shown me that responsiveness on this matter.

Mr David Hanson: I think I speak for the Committee when I say that we have picked up a slight nervousness among them that they can deliver on time and on budget and have cost recuperation. It is important that there is clarity from the Home Office that what you are requesting can be delivered.

Theresa May MP: I believe that the discussions that we have had show both the technical feasibility of, and the ability to deliver on, this capability, but if the Committee would like some further written evidence from the Home Office on that, we can certainly provide that.

The Chairman: That would be very useful. Mr Hanson has put his finger on a problem that came up during the various sessions with communications service providers. They were troubled about costs and whether they had the capacity physically to store the data, including

buildings. You say that you are in continuous discussion with those companies. It would be very useful if we could have some detail. Thank you very much.

Mr David Hanson: The second issue on data retention that has been raised with us is the question of a security risk. Balanced against that, we recognise that large banks, Tesco and Google have massive amounts of personal data on individual citizens that is kept perfectly secure. However, I would welcome your assessment of how you anticipate key data on internet connection records being kept secure by third parties from, for example, cyberattack or internal leaks from individuals within that system. Again, that goes crucially to the centre of the concerns that have been expressed about what is a very compelling argument for that information to be kept.

> ***Theresa May MP***: Indeed. I fully accept the importance of the issue of security for people in relation to the data that will be kept. We make clear—and it will be clear in the code of practice—the importance of ensuring that there is that degree of security. As I indicated earlier, there are already safeguards in place in relation to data security. There is the requirement to comply with the Data Protection Act 1998 and the Privacy and Electronic Communications Regulations 2003. That requirement includes ensuring that there is appropriate security of data. Communications service providers will also be subject to data retention notices, which must comply with the requirements in the Data Retention Regulations 2014, the data retention code of practice and any specific security requirements that may be in the notices themselves. All those requirements will be replicated in the Bill, the codes of practice and the notices that are issued to the companies, so there is a requirement on the CSPs to maintain an appropriate degree of security. Of course, the Bill provides effective oversight by the Information Commissioner, which can ensure that data is held securely.

Mr David Hanson: A particular concern has been raised with us about what we will call third-party data, which is information that businesses would not normally keep for their own business purposes but that it is now suggested they keep. I wonder how the Home Office will assure CSPs that they are not required to retain third-party data. Can we get some clarity around that particular issue?

> ***Theresa May MP***: We have made it very clear that we will not require CSPs to retain third-party data. When I talk about third-party data, I am talking about services that run across their network but that they themselves do not provide. This is a key difference between this legislation and the draft Communications Data Bill of 2012, in which we proposed that third-party data should be retained by CSPs. It has always been possible for public authorities to acquire third-party data, where it is held by CSPs for business purposes or where they can extract it on a forward-looking basis. That can be beneficial in investigations, but they are not obliged to comply with the requirement to extract third-party data where it is not reasonably practical for them to do so. The concern that the companies raised specifically with me was the suggestion that they should have to hold data that was going across their networks and related to services that they did not themselves provide. We are not requiring them to keep that data.

Mr David Hanson: I have one final question. How will the Home Office enforce data retention by those providers that are offshore from the United Kingdom?

Theresa May MP: There are certain aspects of this legislation where we are looking at extraterritoriality. However, there are requirements that we will issue. As you know, data retention notices will be issued to communications service providers in relation to the requirement for them to hold data in a way that enables that to be accessible.

Suella Fernandes: Following on from the point raised by Mr Hanson about cost and the estimates that have been provided by the Home Office, could you set out and explain to what extent the Home Office has engaged with the ISP Association and individual CSPs, and whether or not the estimates are born out of those discussions?

Theresa May MP: Yes. Some interaction with communications service providers has been done on a collective basis, but there have also been discussions with individual communications service providers. There is a recognition that, for individual providers, there may be some aspects of their business that they would not necessarily wish to discuss in front of others. It is from those discussions that we have the confidence that we have in relation to the ability to provide this access to internet communication records.

Suella Fernandes: Traditionally, large CSPs will incur very different costs and burdens to small CSPs, so recovery is granted on a case-by-case basis. Is that right?

Theresa May MP: Yes. We will look very carefully at those CSPs on which the requirements are placed. It would be helpful if notices could be served on some small CSPs that have a very specific niche in the market or specific geographical coverage, but obviously we will look at the necessity and proportionality of that on a case-by-case basis.

Q268 Matt Warman: My question is a follow-up to that, in many senses. Obviously we would expect a retention notice to be served on the largest providers and some specific smaller ones, but some of the smaller ones have expressed uncertainty about whether the expectation is that they should stand ready to be served with such a notice or whether there is a standard that they can reasonably expect to escape, if they are quite small. I do not expect you to say that anything below a certain size will never be touched, but will there be a deterrent effect? Will there be any clarity on that?

Theresa May MP: There is not an intention to describe a CSP that would never be served with a data retention notice, precisely because of the point that I made in response to Ms Fernandes—that it may be that a smaller CSP covers a particular geographical area or a particular niche in the market. We would not look to describe a CSP on which a data retention notice could be served and a CSP on which a data retention notice could not be served. We have to have that degree of flexibility. Wherever the intention is to serve a notice, of course, there is a discussion with that company about its ability, the requirements that might be needed and the technical feasibility of those requirements. We are required to look at the technical feasibility, the costs and any other impact on the CSP. Of course, we are introducing the right of appeal for the CSP, when a notice is served on it.

Q269 Matt Warman: Is it your understanding that a CSP might include things such as people running a wi-fi network in a coffee shop? That is the example that is often used. Do you understand that those would definitely be included, potentially? Could you talk a little about the justification for those sorts of retention notices?

Theresa May MP: Yes. That is left open—and rightly so. If you look at how people are conducting their business, their interactions and their communications today, they are doing that on the move and in a whole variety of settings. It may very well be that there are circumstances where it is appropriate to have that discussion and, potentially, to ask for information to be retained. It is about having that flexibility.

Matt Warman: Might those private networks include university networks or company networks, for instance?

Theresa May MP: I do not think that it would be right for us to exclude any particular type of network, because of the way in which people conduct their business and their interactions these days. However, for any individual decision, there is an onus on the Home Office to look at the necessity and proportionality of that, the technical feasibility of that, what the costs would be and what the impact on that particular CSP or network would be.

Lord Butler of Brockwell: Will the fact that you are having discussions with CSPs or ISPs—and, indeed, the serving of notices on them—be a confidential matter?

Theresa May MP: The serving of notices on them would be a confidential matter. We would not look to make that a public matter. For obvious reasons, when one is looking at the reasons why we should have access to this data and, therefore, require its retention, I would not want to suggest that there are particular CSPs that people could migrate to purely because a retention notice has not been issued on them.

Lord Butler of Brockwell: That is what I had in mind. Would it be possible to maintain that confidentiality if, for example, you were going to bring proceedings against them? Would they be immune from applications under the Freedom of Information Act, if you were asked on which providers notices had been served?

Theresa May MP: I will check the issue on the Freedom of Information Act, if I may. Obviously there are some elements of exclusion under the Freedom of Information Act in relation to national security matters, in particular, as well as some matters relating to law enforcement. I am very happy to write to the Committee with more specifics on that point.

Dr Andrew Murrison: Can I ask a little more about so-called coffee shop ISPs? Most of us would be comfortable with the process affecting CSPs, since they tend to be larger operators, but potentially there is cause for some very small operators to feel distinctly threatened by all of this—and, possibly, to be targeted by the process. Can you be absolutely clear that the costs that will bear on those small operators will not be disproportionate?

Theresa May MP: As I indicated earlier, we are operating on the basis of cost recovery, in relation to the Government providing some funding in these areas. In looking at and having the discussion with a particular provider in relation to retention of this data, the issues of the impact on that provider—the costs—would be taken into consideration. Of course, that would be balanced against what the expectation would be with regard to the necessity of access to data. Those sorts of considerations would be entered into.

Q270 Dr Andrew Murrison: Can I press you on the vexed issue of encryption? Most of us who use the internet would probably regard end-to-end encryption as a very good thing.

Indeed, many CSPs use it as part of their business model. In general, security is promoted by encryption, yet the Bill talks about "removing electronic protection". We have heard terms such as "establishing a back door" for the agencies to access information. Clearly, there is a threat that businesses that wish to conduct their operations with a degree of privacy may note the relative prurience of the British system, as articulated in the Bill, and choose to move their businesses outside, if they cannot guarantee to their customers the sort of privacy that other Administrations can. Could you give us some indication of what you mean by "removing electronic protection" and what the implications of that are for end-to-end encryption? Could you also outline any worries that you may have about the apparent intention of this Bill to end the degree of security guarantee that applies in the UK at the moment?

Theresa May MP: I am grateful for the opportunity to provide a degree of clarity, I hope, around the issue of encryption and what we are proposing on that in the Bill, because there has been some commentary that has not accurately reflected what we are intending to do in the Bill. As a Government, we believe that encryption is important. It is important that data can be kept safe and secure. We are not proposing in the Bill to make any changes in relation to the issue of encryption and the legal position around that. The current legal position in respect of encryption will be repeated in the legislation of the Bill. The only difference will be that the current legal position is set out in secondary legislation and it will now be in the Bill. We say that, where we are lawfully serving a warrant on a provider so that they are required to provide certain information to the authorities, and that warrant has gone through the proper authorisation process and is entirely lawful, the company should take reasonable steps to ensure that it is able to comply with the warrant that has been served on it. That is the position today, and it will be the position tomorrow under the legislation.

Dr Andrew Murrison: CSPs will then say, "Because we have end-to-end encryption, we are unable to help you with that". Can I press you a little more on what removing electronic protection would mean in practice?

Theresa May MP: What we say to companies today and will say to companies under this legislation is that, when a warrant is lawfully served on them, there is an expectation that they will be able to take reasonable steps to ensure that they can comply with that warrant—i.e. that they can provide the information that has been requested under that lawful warrant in a form that is legible for the authorities.

Dr Andrew Murrison: So you are not looking to them to provide a back door for the agencies or a key, as it were.

Theresa May MP: No. We are not saying to them that the Government want keys to their encryption—no, absolutely not.

The Chairman: You want translation, in a sense, so that whatever information the warrant demands is readable by those who need to read it.

Theresa May MP: Yes.

The Chairman: But the company's encryption facilities would be safeguarded.

Theresa May MP: Yes. The Government do not need to know what the encryption is or to know the key to the encryption. It is exactly as you say, Chairman. If there is a lawful warrant requesting certain information, it is about that information being readable.

Q271 Lord Strasburger: Good afternoon, Home Secretary.

Theresa May MP: Good afternoon.

Lord Strasburger: Can we move to the vexed question of the many bulk powers that are in the draft Bill? Those involve large-scale state hacking, surveillance and copying of data, which, to a very large extent, belongs to people who have no involvement whatsoever in crime. We have heard from the security and intelligence agencies and a few other witnesses that those powers are useful and necessary, but a much larger number of witnesses and written submissions—by no means only from civil society groups—have argued strongly that these powers are overly intrusive, disproportionate and so are illegal under EU law. My first two questions are: can bulk powers ever be deemed proportionate, and on what basis does the Home Office believe that these mass surveillance powers will be seen as legal in the context of recent European court decisions?

Theresa May MP: I am tempted to say, Lord Strasburger, that, by definition, my answer to your first question has to be yes, precisely because there are powers that exist today in relation to bulk matters, and those will be within the legislation. It is the case that there are occasions when this is proportionate. Of course, we have seen challenges in the European courts in relation to the question of data retention, which led to the Data Retention and Investigatory Powers Act 2014. In relation to those matters, we believe that what we have put in our DRIPA legislation and what we will bring into this legislation meets the requirement. I do not think it is clear that the European Court of Justice judgment intended to impose minimum standards. We believe that our current regime is compliant with the requirements of EU law and that the regime that we are proposing and the legislation that we are bringing forward are similarly compliant with EU law. As you know, there has been a test case in relation to DRIPA in the UK courts. The Court of Appeal also agreed that it was not clear that the European Court of Justice intended to impose minimum standards in relation to these matters and has decided to refer questions about the interpretation that has been taken of the case with the ECJ—the Digital Rights Ireland case—to the European Court.

Lord Strasburger: I guess that time will tell. There is a risk that the Bill, if it becomes an Act, will be overtaken by something that happens in the courts, but time will tell.

We have also heard from many witnesses that bulk powers are operationally counterproductive, because agency analysts are being blinded by the huge volumes of data that are being collected. We have also heard that the problem will get much worse, because in 10 years' time the massive quantities of data will have increased by a further factor of 1,000 or more. For almost every recent terrorist attack in the West, one or more of the perpetrators was previously known to the intelligence agencies and was somewhere in their database, yet they were not picked up as an imminent threat by the analysts, who are drowning in data.

We heard last week from a former NSA technical director that the very expensive approach of the NSA and GCHQ—namely collecting all the data all the time—causes the agencies to

miss opportunities to prevent attacks. That means, we were told, that avoidable deaths will occur in the future and that 9/11, 7/7 and both Paris attacks could have been prevented. He and others argue for a much more targeted collection of information, which works because analysts see manageable quantities of data that still includes the bad actors they are looking for.

My question is, what do you think of making it more likely that we will find the needles by shrinking the haystack, with smart, targeted collection?

> ***Theresa May MP***: May I pick up on a number of the comments that you made in your question, Lord Strasburger? First, I must challenge your reference to the UK authorities "collecting all the data all the time". We do not collect all the data all the time. I wish to be very clear with this Committee that that would be a misdescription and a misrepresentation of the action of the UK authorities.
>
> I would also remark on your references to a number of terrorist attacks that have taken place and the comment that you say somebody made to the Committee that those could have been prevented. The inquest on 7/7 that took place under Lady Justice Hallett was very clear in its findings, which were of a different nature from what you have suggested in relation to that.
>
> To put a very simple point, which is a point that a former Home Secretary—not, as it happens, from my party—used to make, "You cannot look for the needle in the haystack unless you have got the haystack". In some cases, you need to be able to access this data to identify it. There are a variety of ways in which the agencies are careful and look to target how they deal with data. However, if the suggestion is that you cannot collect any bulk data or have access to any bulk datasets whatsoever, you will miss the opportunity. I do not see that that helps you to deal with the circumstances and issues that you are raising.

Lord Strasburger: You and I have discussed haystacks in the past. The evidence we heard last week was that the haystack now is so big that although we know that data about the perpetrators of those texts that we have mentioned was in there—we know that is the case—it was not picked up and identified as a threat by the analysts. The suggestion from Mr Binney last week, who is not an inconsequential witness being the technical director at the NSA, was that the reason they were missed was because the analysts who were supposed to spot them were drowning in too much data that was nothing to do with what they were looking for. I only report to you what we were told last week.

> ***Theresa May MP***: Yes; I was looking through that. I knew I had the reference to what he said here. First of all, as I indicate, it would be wrong to give the impression that we are collecting all of the data all of the time. Once again, I want to be very clear about that. But bulk capabilities are important because, if you are going to be able to investigate a target, you need to be able to acquire the communications in the first place. When the target is overseas, bulk interception is one of the key means, and indeed may be the only means, by which it is possible to obtain communications. It is not the case that it is always used in an untargeted way. Once again, I would challenge that in relation to these issues.
>
> When particular incidents have taken place, of course we look at the systems that are in place to ensure that we can make the way we operate as effective as possible. There is a

very fundamental reason for being able to have access to this information and being able to deal with this information. It is about keeping people safe and secure.

Lord Strasburger: Finally, on mass surveillance, Home Secretary, we have seen an operational case for internet connection records but we have not as yet seen one for bulk acquisition of communications data, bulk equipment interference, bulk interception and bulk personal datasets. These powers have been used for some time, despite not being revealed until 2015 and never having been approved by Parliament. In a supplementary paper just a few days ago, David Anderson warned, "If an evidence-based public defence of these powers is not attempted, the argument may yet be won at the European level by those who assert the powers to be either useless or more sinister in their operation than is in fact the case". My question is: when will the missing operational cases be published?

Theresa May MP: I am sorry, Lord Strasburger, but again I want to challenge one of the phrases you used in your question to me. You indicated that what we were doing was mass surveillance. You described it as mass surveillance. The UK does not undertake mass surveillance. We have not undertaken, and we do not undertake, mass surveillance. That is not what the Investigatory Powers Bill is about.

You referred to bulk equipment interference. This is important. There will be cases where it is necessary to use that in order to be able to keep pace with those who want to do us harm, where it is not possible to disrupt and intervene on activities through interception, for example. If you are asking me to write to the Committee to give a further explanation of why I think the bulk powers are necessary, of course, Chairman, I can do that, but I would wish to be very clear that mass surveillance is not what we are talking about.

Lord Strasburger: I accept you are very clear about that. I want to be very clear about the fact that these four powers have never been before Parliament—ever. I did a search of Hansard. If you look for "equipment interference" or all the other terms I have just mentioned, they are not mentioned until 2015, and one of them just two months ago by you. It is rather important, now that they are coming before Parliament for the first time, that there is a proper justification and explanation of what is involved, what the liberty and financial costs are and so on. We have had it for internet connection records, but for some reason we have not had it for the other four. I am just asking that the Home Office publishes an operational case for it. Mr Anderson says that it is very much in the Government's interest to do so, because without those operational cases the Government are going to run into a lot of trouble in the European courts.

Theresa May MP: One of the aims we have had in relation to the Bill, which I have been very clear about on the Floor of the House, has been to give a greater degree of transparency and clarity to people of the powers to which the authorities do have access—

Lord Strasburger: I congratulate you for that.

Theresa May MP: —and the legislative framework for that. One of the purposes of having the processes of scrutiny that we have had on the Bill is precisely for these issues to be looked at, which is why, as I indicated earlier, I am grateful for the work of this joint scrutiny committee. There are a number of reasons why it is important to have these

various bulk powers. I have given a number of references here, but I am very happy to put that in writing to the Committee.

Q272 Lord Strasburger: Turning to bulk personal datasets, the lack of clarity about them has been a concern for many witnesses and Committee members. We understand that there are databases that exist in the public and private sectors and that each contains personal information about potentially millions of innocent citizens. We also understand that the security intelligence agencies have for some time been getting copies of this data, either with or without the owner's permission, and once again without the explicit approval of Parliament for them to do so. Some witnesses have told us that these datasets have been medical records, bank account data and other highly personal information. In order to establish the truth about bulk personal datasets, the Committee has asked the Home Office many times for a list of them, which has been refused on every occasion. My question is: how can the Committee form a view on the appropriateness of the secret ingestion of bulk personal datasets without having any idea what they are?

Theresa May MP: I understand, Chairman, that the Security Minister has written to the Committee today on this matter, explaining why it is the case that we do not list out the various bulk personal datasets to which access is provided. I am happy to give you examples. I think everybody would accept that a list of people with a firearms licence would be very useful if you are looking at people who are of particular concern to law enforcement and the agencies, to be able to see who has access to firearms. The letter that has been sent today—and I fully recognise that it may not have been possible for members of the Committee to have looked at it yet—sets out why it is the case that we do not list out every single personal dataset that may be accessed. I think it is important for us to do so, and we are very clear in a number of areas that it is important for us to retain that degree of flexibility precisely because of the sort of people that we are dealing with.

Lord Strasburger: It is not possible to exclude certain datasets like medical records.

Theresa May MP: No. As soon as you start excluding certain datasets, that gives messages to those who would seek to do us harm about the way in which the authorities operate.

The Chairman: It was an issue that exercised the mind, for example, of the Information Commissioner when we questioned him last week. Three other members of the Committee want to come in on these issues. I would ask them to be reasonably concise because we have to move on to authorisation. Dr Murrison, Ms Atkins and Ms Fernandes, please be concise.

Dr Andrew Murrison: I will be brief. Home Secretary, I want to press you on this issue of the nature of the datasets. It seems to me that there is a continuum at one end of the sort that the Home Office has very helpfully told us they would be focused on. You have mentioned firearms certificates, passport applications, electoral roll material and telephone directory stuff. Some of it is in the public domain already, of course, which is very innocuous and which I suspect the public would have absolutely no difficulty with at all. At the other end, there is stuff that may not actually be public record at all, either explicit or private. I am thinking of things like medical records—which are increasingly important as we move towards electronic medical records—clinic attendance and bank accounts. Those are highly sensitive things. What would be reasonable without being specific, and I accept the reasons

for not being specific, is for you to say where on that spectrum you would expect attention to be focused and cut off. It is important that people do know whether in fact the intention of this legislation is to tap into very personal material of the sort I have described at the far end of the spectrum, or whether you feel that your attentions will be focused and sighted specifically in this Bill or through codes of practice. It is important that we have some better sense of where this is going to fall, other than from what you have already provided us with.

> ***Theresa May MP***: If I may, Dr Murrison, I would approach the issue from a slightly different angle. What we are doing in the Bill is not listing out the datasets but providing for a greater degree of safeguard in relation to the acquisition of datasets through the warrantry process with the double-lock authorisation on the warrantry process. The fact that these datasets are available and are accessed is something that is looked at in the current oversight arrangements by the relevant commissioners. They have recognised that this is an important capability. It is also the case that the Intelligence and Security Committee can scrutinise any classified elements in relation to this to provide this Committee with greater reassurance, if that is helpful. As I say, the important thing is to know that these are being accessed in accordance with safeguards and authorisation processes that ensure that double lock, which will be the case in terms of warrants for bulk personal datasets, and which ensure their necessity and proportionality.

Dr Andrew Murrison: What would at least be helpful is if you could say whether or not the four examples I have just given would be typical of the sort of thing you would expect to be collected through this process, as opposed to simply being examples. You will appreciate the clear difference between the two.

> ***Theresa May MP***: I do, but, as I have indicated in response to Lord Strasburger and has been indicated by the Security Minister in the response to the letter, which I recognise that not all members of the Committee may have had an opportunity to see, we do not feel it is right to go down the route of giving information about the sort of datasets that would be acquired and the sort of datasets that would not be acquired. You are asking me, I think, what is, in a sense, a less specific version of the question that Lord Strasburger asked me, which is why I am giving you the same answer. The important thing in relation to the privacy angles and in relation to ensuring that the authorities are only doing what is necessary and proportionate here is the fact that there will be a warrantry process that will have that double-lock authorisation in it. There will be an oversight process that provides that safeguard for people.

Victoria Atkins: Lord Chairman, this is really a point to clarify the evidence that was given last week by Mr Binney. Lord Strasburger has not mentioned it, but I think it is important that it is on the record given that this is being televised and there are members of the Committee who were not in that evidence session. Mr Binney conceded that he was last cleared for security with the NSA 15 years ago, and his evidence at the end was that he was accusing all the law enforcement officers and security service officers of being wrong in their evidence to this Committee, and possibly misleading this Committee. I think it is important to put that in context when Lord Strasburger cites Mr Binney's evidence. It will be a matter for the Committee in due course to decide the weight to attribute to Mr Binney's evidence.

Suella Fernandes: I have two simple questions. Home Secretary, in the context of the access to bulk data, do private companies like large retailers, charities and other technological companies have bulk access to data, to your knowledge?

> ***Theresa May MP***: There are bulk personal datasets that are in the public domain and to which I am sure organisations other than Government have access.

Suella Fernandes: It is part of our digital society, is it not? Lastly, bulk access differs from bulk use of data. What safeguards and limits are in place on the use of bulk data in this regime?

> ***Theresa May MP***: I am grateful. Obviously, we talk about various aspects of bulk data and we have just been talking particularly about bulk personal datasets. We have talked about the bulk powers. There are provisions in this Bill, as I have indicated in relation to bulk personal datasets, that introduce an authorisation process that I hope would provide greater safeguards and therefore give greater reassurance to people in relation to how it is possible to access some of these bulk datasets.

Suella Fernandes: Does this Bill represent a codification and clarification of practice, in your opinion?

> ***Theresa May MP***: What we have tried to do in this Bill is to be transparent and clear about the powers that are available to the authorities, and crucially to bring powers into one place, into one piece of legislation. One of the comments that was made in the general debate that we had on this matter in the House of Commons was that there was a concern that the current legislation was in different places. We have brought the legislation together and aimed to be transparent and clear so that people can see the sort of powers that the authorities have and are able to use but they can also see the safeguards that are available to them. I think this is world-leading legislation precisely because of that balance that it creates.

The Chairman: Thank you very much. We now move on to the very important area of authorisation with Lord Hart.

Q273 Lord Hart of Chilton: Home Secretary, this is a question about the powers of the Judicial Commissioner in authorising the various issues given for authorisation under the Bill. Some have said that the powers of the judge are too narrow and are really no more than process checks. Others, including David Pannick, have said that the judges applying a judicial review test must themselves consider the merits and decide whether the measure is indeed necessary and proportionate. Your department has said that in relation to the authorisation of warrants: "The specifics here are that two things will be critical: first, that they decide in the first place that the action is rational and lawful; and, secondly, that it is necessary and proportionate. Those are exactly the same tests as the ones the Secretary of State will be looking at". If it is the case that the Judicial Commissioner will be applying the same test as you, why does the draft Bill specify judicial review test principles?

> ***Theresa May MP***: One of the advantages that one has with judicial review principles is that it gives the Judicial Commissioners a degree of flexibility as to how they approach particular cases depending on the impact on the individual of what it is that they are

looking at. They will be able to make an assessment and a judgment as to how they wish to approach the evidence that is before them. The Secretary of State looks at the necessity and proportionality of the warrantry. It will be open to the senior High Court judge to look at necessity and proportionality, but under the judicial review provisions they will have the flexibility to determine the way in which they look at that decision. I think that was one of the points that Lord Pannick was making in the article that he wrote before Christmas.

Lord Hart of Chilton: So it would not be right to suggest that the judicial review principles are there in order to prevent a judge from second-guessing the Secretary of State on the merits.

Theresa May MP: No. It will be up to the judge. These will be people who will be well versed in judicial review principles and in exercising those principles. It will be up to them to determine how they approach any particular issue. There may well be circumstances in which they might apply a lighter-touch approach to reviewing a Secretary of State's decision, and others in which they will look more at necessity and proportionality.

Lord Hart of Chilton: It would not come as any shock to you if a particular judge in a particular case, looking at it from his point of view, decides that he would substitute his decision for yours and look from that point of view at the merits of the case.

Theresa May MP: The whole point of the double-lock authorisation is that both parties have to agree to the warrant being applied. If the Judicial Commissioner decides that the warrant should not be applied, having looked at it and applied the tests that they need to apply, then obviously it cannot be operated.

Lord Hart of Chilton: That then would be a true double lock. It would not be a true double lock if the judge was precluded from imposing his decision over yours, because he was looking at the merits and deciding that you had come to the wrong decision, not because of some error or law or—

Theresa May MP: Lord Pannick also noted in his article that judges do accord the Executive a margin of discretion to reflect the expertise in national security matters.

Lord Hart of Chilton: Of course, particularly in national security.

Theresa May MP: They are not re-taking the decision. They are looking to see whether the original decision was flawed. There will be circumstances in which they will determine how they apply that test under the judicial review principles, but it does give them the flexibility to determine that perhaps in one case they might look at it with a lighter touch than they would in another. It is a genuine double lock in that both parties have to agree in order for the warrant to be applied.

The Chairman: Last week, 12,000 miles away at ten past five in the morning, the New Zealand Commissioner—a former High Court judge—who would be the double locker, if you like, in the New Zealand system, said that when he came to applying his mind to a warrant he was not necessarily thinking, "I am a judge and I am going to look at it as a judge", but he was going to look at the necessity and proportionality as well. What you are saying, Home Secretary, is that, essentially, a judge could, and might, look at it in that way too.

Theresa May MP: It will be for the Judicial Commissioner to determine whether the facts of a particular warrant merit the more rigorous review, which could include some consideration of necessity and proportionality.

Dr Andrew Murrison: Thank you for that, Home Secretary, because I think that has reassured a lot of us. Therefore, would it be unreasonable to look at Clauses 19(2) and 90(2), which speak of judicial review rules, since, if we are approaching this on the basis of almost co-equality between the Secretary of State and a Judicial Commissioner and allowing the Judicial Commissioner to have a merits-based approach to this, it would appear that that stringency becomes redundant?

Theresa May MP: The purpose of having the judicial review principles is that it provides the flexibility for the Judicial Commissioner to determine the degree of assessment that they choose to put on a particular application. This was one of the points that was highlighted by Lord Pannick. We are not precluding the possibility of a Judicial Commissioner deciding that they want to give a more rigorous review of a Secretary of State's decision, but they could also determine that in a case they wanted to apply a lighter touch. I am trying not to tie them down, if I can put it like that. They get a degree of flexibility with reference to the judicial review principles.

Baroness Browning: Home Secretary, I would like to ask you about urgent warrants, but, before I do, could I pick up on a couple of points following on from Lord Hart's question? Notwithstanding that the judges appointed as Judicial Commissioners will be very familiar with judicial review principles, would you none the less expect them to receive any kind of training on their appointment? Would they also be subject to any form of appropriate vetting procedure?

Theresa May MP: The individuals who will become Judicial Commissioners will be picked from a group of people who will already have been through certain degrees of checks by virtue of the fact that they have been in the judiciary and are senior members of the judiciary. What was the first question you asked me?

Baroness Browning: Whether they would need any training.

Theresa May MP: I would not expect simply to introduce Judicial Commissioners and sit them in front of these things without some degree of training, which would be explanations about the processes that are gone through in terms of warrantry and things like that.

Q274 Baroness Browning: Thank you. Can we move on to urgent warrants? Why does the draft Bill allow five days for a warrant granted under urgent circumstances to be reviewed by a Judicial Commissioner? Assuming that they are appropriately resourced, why is the period for retrospective review not significantly shorter? Five days seems a very long time.

Theresa May MP: I recognise that there has been some comment on the issue of five days. When RUSI produced its report, I think its suggested that the period that is set should be 14 days. Five days is the current period for any emergency warrant. It automatically has to be reviewed after five days, so five days has been put into the Bill. I am very happy to look at that period of time if that is an issue that the Committee wishes to bring forward.

Q275 Victoria Atkins: Home Secretary, I am dealing now with interception warrants and, first, the issue of modifying interception warrants. Currently, under the Act, when such warrants are modified, those modifications are not subject to judicial authorisation. What safeguards exist to prevent this from being used to sidestep the double lock?

Theresa May MP: There is a limit to what can be considered to be a modification of a warrant. There might be more minor modifications or slightly more significant modifications. The sort of modifications might be the addition of a device to a warrant, for example. The necessity and proportionality of a warrant against a particular individual will have been determined by the double-lock authorisation process. Anything that was in that order would not count as a modification. Anything that required a warrant against a particular individual would require the double-lock authorisation process.

Q276 Victoria Atkins: For my second question I am going to ask you to use your draft Bill because this is a complicated set of sentences that I have to put to you. The first concerns Clause 13(2)(a), which reads: "A targeted interception warrant may relate to a group of persons who share a common purpose or who carry on, or may carry on, a particular activity". Would you keep a finger in that page, as it were, and move to Clause 83(1)(f)? That clause reads: "A targeted equipment interference warrant may relate to equipment that is being, or may be being used, for the purposes of a particular activity or activities of a particular description". It is a very legalistic way of saying, "Could this be used, in effect, to create thematic warrants that could apply to a very large number of people and therefore cannot be classed as targeted?"

Theresa May MP: The answer is no. It will not be possible to use a thematic warrant against a very large group of people. The purpose of a thematic warrant is, for example, circumstances in which perhaps somebody has been kidnapped or there is a threat to life, where only certain information is available, and it is necessary because of the pace at which something is developing to identify the group of people who are involved with that particular criminal activity as being within the thematic warrant.

Victoria Atkins: What would the difference be between such a warrant and a bulk interception or equipment interference warrant?

Theresa May MP: Are you now talking specifically about Clause 83 as opposed to Clause 13(2)(a)?

Victoria Atkins: Yes; this is a lawyer's paradise.

Theresa May MP: I am looking a little surprised because, as I see it, there is nothing in Clause 83 that suggests that what is being looked at is a bulk equipment interference warrant.

Victoria Atkins: That is the point. Thank you very much.
Lord Butler of Brockwell: This is on authorisation again. There has been some attention among our witnesses as to the differences between the procedure for authorisation of warrants and modification of warrants between the intelligence agencies and law and order. This relates to equipment interference and it carries on from the question about interception. In the case of equipment interference warrants, the intelligence agencies require a warrant from the Secretary of State plus the Judicial Commissioner, and with law enforcement

similarly it has to be a chief officer and the Judicial Commissioner. In the case of modifications, it is different. For intelligence, it is not subject to approval by the Judicial Commissioner, whereas for law and order it is. What is the reason for treating modifications of warrants differently between the agencies and law and order?

Theresa May MP: With regard to modifications to the different warrants from either the agencies or from law enforcement, modifications to the agency warrants require approval from the warrant issuer, which is the Secretary of State or designated official, so that they are being looked at independently from the agency. Where there is modification to law enforcement—and I may have missed the point of the question—the issuing authority is the internal law enforcement chief. To give the independence, that is why we have instructed that the Judicial Commissioners should also authorise modifications for law enforcement equipment interference warrants. It is about getting that degree of independence but it can be achieved in different ways.

Lord Butler of Brockwell: I see, but I wonder why there are different ways.

Theresa May MP: In relation to the agencies, the process is the one that exists at the moment, on which there have been no concerns expressed as to how it operates. As I indicated in response to Ms Atkins, when we are talking about modifications, we are not talking about something that opens up a whole new warrantry in relation to, say, an individual, but it might be something like another device being placed on the warrant.

Q277 Lord Butler of Brockwell: Thank you. In the case of the technical capability and national security notices, these are not subject to the double lock. Why not?

Theresa May MP: The double-lock authorisation is there where there are processes that are intrusive into an individual. When you look at the technical capability and national security notices, those are of a different order. They are not about that question of the intrusion that is taking place into an individual.

Q278 Stuart C McDonald: I have one or two questions about extraterritoriality, please, Home Secretary. A number of witnesses, both in their written and oral evidence, have expressed concern that there is not very much in the Bill about these issues. First, dealing with the question of the UK sharing information abroad, what safeguards are there to limit what can be done in that regard?

Theresa May MP: We look at the handling arrangements that are in place when we are sharing material with overseas partners. It is Clause 41 of the draft Bill that sets out that, before intercept material is shared with an overseas authority, the issuing authority sharing the material must be satisfied that they have appropriate handling arrangements in place to protect the material, equivalent to those that apply under Clause 40. Those might not be exactly mirrored; they might not be absolutely the same; but they are equivalent, so they give the same degree of appropriate handling arrangements.

Stuart C McDonald: But it is a matter for the appropriate issuing authority to decide. Is that not quite weak? Can we not strengthen that in the Bill?

Theresa May MP: We are confident that the appropriate issuing authority has this requirement on them and therefore will ensure that these are in place. I recognise that the joint scrutiny committee will be reporting.

Stuart C McDonald: Thinking of things the other way round—the United Kingdom obtaining material obtained through interception overseas—am I right that that is essentially going to be down to codes of practice? Again, there is a lot of criticism that that is not satisfactory.

Theresa May MP: Do you mean in terms of the United Kingdom issuing warrants in relation to an overseas provider?

Stuart C McDonald: Yes. The evidence of Amnesty International, for example, is that there are no provisions at all in the Bill dealing with the receipt by the United Kingdom of material obtained through interception by overseas partners other than in Schedule 6. Schedule 6 provides a bare statement that codes of practice will "cover the process" for overseas requests and handling data received from them. Is it down to the codes of practice, essentially, to govern that?

Theresa May MP: There will be codes of practice. The reason I asked the question was to try to clarify exactly what sort of circumstances we are talking about in terms of extraterritoriality.

Stuart C McDonald: Interception.

Theresa May MP: In relation to an interception, we repeat the position that we put into DRIPA that has always been asserted by all Governments in relation to the ability to exercise a warrant against a company that is offering services in the United Kingdom and binding them by the law of the United Kingdom. That will be a lawful warrant that would be applied to a provider. Information obtained under that warrant would be similar to information obtained under a warrant that was issued domestically.

Stuart C McDonald: I think these witnesses are getting at information that was obtained by security and intelligence services of other countries. Correct me if I am wrong, but, unless the Bill says something about this, there could be protections that prevent our security and intelligence services obtaining information on certain people because of all the protections that you have set out in the Bill. It would drive a coach and horses through the Bill if they were then able to simply go and obtain this information from the security intelligence services of neighbouring countries. Is there anything in the Bill that governs how these relationships work?

Theresa May MP: We have been very clear in ensuring that where information is obtained it is done so against an appropriate legal framework. There are provisions in place that ensure that the agencies operate and only obtain information where it is lawful for them to do so.

Stuart C McDonald: Where do we find that legal framework? Am I right in thinking it is all down to international treaties, some of which we know about and some of which are perhaps not in the public domain?

Theresa May MP: There are various aspects to the legal framework against which the agencies operate. If I can be of more help in writing to the Committee—

The Chairman: Thank you, Home Secretary. I am going to have to move on now—because I know you are pressed on time—to privilege with Lord Hart.

Q279 Lord Hart of Chilton: It will not surprise you at all to know that there have been many who have complained of the limited protection for legal privilege and for journalistic sources. I want you to explain to us why it is that you cannot put legal privilege, which plays an important part in the rule of law, in the Bill itself rather than relying upon a code of practice, which as yet is unpublished. Dealing first with legal privilege, why is that necessary?

Theresa May MP: It is important that the law enforcement and the agencies are able to use these powers in circumstances where it is necessary and proportionate for them to do so and not to exclude the use of these powers in any particular sets of circumstances. You mentioned both legal professional privilege and the question of journalistic sources. Of course, we are making specific provision for certain circumstances in relation to journalistic sources, but the significance of the relationship between an individual and lawyers in discussing matters is always recognised. I do not think it would be right to say that these powers could never be applied in those circumstances. It is right that, again, it is a question of judgments about necessity and proportionality.

Lord Hart of Chilton: There is not much evidence base in all of this. How many times has the Home Office had to interfere with legal privilege? How many times has that happened? Is it a very tiny fraction of numbers?

Theresa May MP: You used the phrase "interfere with legal privilege". We are not actively interfering with legal privilege, but I am sure everybody would agree that you could not accept a situation where you said, in regard to anybody who had any legal qualifications and who might be operating in a relationship relating to those legal qualifications with an individual, that these powers could never be used in those circumstances, because, I am sad to say, you may very well find that there are circumstances in which people who are legally qualified and operating in those are potentially providing support to some people who would perhaps be involved in, for example, criminal activities.

Lord Hart of Chilton: Of course, if they misuse privilege, they are not able to call upon it to be used as a defence. It is not a universal rule. If you are a naughty lawyer, you cannot claim legal privilege.

Theresa May MP: Yes, and sometimes it may be necessary to use some of these powers to identify that you are a naughty lawyer in the first place.

Lord Hart of Chilton: I go back to the question: is there an evidence base where you have done this?

Theresa May MP: There is, I think, an important point of principle in the ability for law enforcement and agencies to have these powers and to be able to exercise them in particular circumstances. If we go back to remembering exactly why it is that they have

the ability to exercise these powers, dealing with crime and with terrorists who would seek to do us harm, it is important that these powers are available. We do not publicise figures in relation to particular types of warrants or the interception that is undertaken by those warrants. Indeed, under RIPA, it is an offence to indicate whether a warrant is in place in a particular circumstance or against a particular individual.

Lord Hart of Chilton: The point being made by many people is that for you to interfere with legal privilege it should be on the face of the Bill and not in a code of practice.

Theresa May MP: I think that the arrangements that we are putting in place are appropriate for the reasons that I have set out.

Q280 Lord Hart of Chilton: I will not press you any more on that. The last of the trio of questions in relation to that is that the Wilson doctrine is not enshrined in the Bill and it does not require the Prime Minister to make a declaration to Parliament. Why was that safeguard left out of the Bill?

Theresa May MP: The Wilson doctrine has been recently tested before the tribunal. It was found that the Wilson doctrine was still in place and that the definition of the Wilson doctrine was as I had set out to the House of Commons. The important element of the Wilson doctrine that will be in the Bill is that it will be a requirement, where it is suggested that there be interception in relation to not just a Member of Parliament but Members of the House of Lords, UK MEPs and Members of the devolved assemblies and parliaments, that where that is going to be the case the Prime Minister must be consulted on its use.

The issue as to the aspect of the Wilson doctrine that was about the Prime Minister making a statement to the House when policy changed in relation to the Wilson doctrine is of a slightly different order. The Prime Minister has been clear that that still applies. I do not think it is appropriate to put that on the face of a piece of primary legislation.

Lord Hart of Chilton: I suppose it is part of a subset of accountability to Parliament. If you do not make a statement to Parliament, you have simply considered the question. It is not quite the same.

Theresa May MP: I am not sure whether there is some misunderstanding about the nature of the Wilson doctrine in the statement to Parliament that the Prime Minister makes. The statement to Parliament that the Prime Minister makes is not that there has been the interception of a number of Members of Parliament. The statement that is in the Wilson doctrine is about whether the policy that has been adopted is different. As to how these matters operate, statements about changes of policy on a whole range of matters are regularly made to Parliament. But that is not a requirement that is on the face of any legislation in any area in which we operate.

The Chairman: There are some other questions, but I know your timing is difficult. Are you able to answer any more?

Theresa May MP: Yes, for a short period. I have a speaking engagement on the Estate, to which I will have to go shortly, but I can take a few more.

The Chairman: Ms Mahmood, can you be quite precise, as you always are?

Q281 Shabana Mahmood: I will be, Lord Chairman. On Judicial Commissioners, the system for appointing them by the Prime Minister for a term of three years is different from the way in which other senior judges are appointed. Why is there a difference between the two?

Theresa May MP: The commissioners currently are appointed by the Prime Minister. You are talking about the Judicial Appointments Commission specifically.

Shabana Mahmood: Yes.

Theresa May MP: Yes, there will be some circumstances in which one might be looking at a sitting judge being appointed, in which case it will be a matter more for the Lord Chief Justice and for advice from the Lord Chief Justice. Indeed, the intention is that the Lord Chief Justice would be making nominations to the Prime Minister.

Shabana Mahmood: Are you not worried, given the controversial history of the Bill, with what happened in the last Parliament, that there is maybe the appearance that the Judicial Commissioners might have a reduced sense of independence from the Executive? Is that a concern to you? Is that something you would like to avoid?

Theresa May MP: I recognise the importance of people seeing the independence of the commissioners. The current commissioners are appointed by the Prime Minister. There is no suggestion that they have not been independent in the operation of the work that they have done. I do not believe that the appointment by the Prime Minister would jeopardise in any sense the independence of the Judicial Commissioners in the future. They will, as I say, be people who have been or are senior members of the judiciary, and there will be circumstances in which the pathway with the nomination by the Lord Chief Justice is more appropriate than the Judicial Appointments Commission.

Q282 Shabana Mahmood: Thank you; that is helpful. One of the arguments that has been made to us is that the function of authorisation and oversight being done by the same people might give the appearance that the commissioners are effectively marking their own homework. Is this something that has been put to you? Is it something you are concerned about?

Theresa May MP: We have thought about this issue. We already have an example, through the Office of Surveillance Commissioners, where they are performing two functions. There will be two functions and, therefore, two sets of people within the Investigatory Powers Commissioner and that office—those who are undertaking the authorisation process and those who are undertaking the inspection process. There are some benefits for the ability of those to interact, to understand some of the issues of practice, but it is important that they keep their functions separate. Because we have an example of how that is done already with one of the offices, it is perfectly possible for that to be done in a way that maintains their independence. I am tempted to say, given that we are talking about Judicial Commissioners, that I am sure they will fiercely defend their independence and the necessity of keeping those functions clear.

The Chairman: Thank you very much. We will probably have to stop there as it has been nearly two hours. It has been very informative. It has been exhaustive but I hope not

exhausting. Thank you very much for coming along. We now look forward to compiling our report, which you will see in due time. Thank you very much again, Home Secretary, for coming along.

Theresa May MP: Thank you, Chairman.