Joint Committee on the Draft Investigatory Powers Bill

Oral evidence: Draft Investigatory Powers Bill, HC 651

Wednesday 16 December 2015

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, Lord Butler of Brockwell, Bishop of Chester, Lord Strasburger.

Questions 162-196

Witnesses: **Detective Superintendent Paul Hudson**, Head of the Metropolitan Police Service Technical Unit, **Michael Atkinson**, Secretary to the National Police Council's Data Communications Group, and **Temporary Detective Superintendent Matt Long**, Child Exploitation and Online Protection Command at the National Crime Agency, gave evidence.

Q162 The Chairman: A very warm welcome to all of you. I was just saying that this is a rather large room—a bit like Mussolini's waiting room, if you ever saw that. You are miles away down there. Can I say how valuable the Committee thought our visit was yesterday, by the way, as an introduction? It was extremely useful and gave us a lot of food for thought. I am going to start the first question and my colleagues will come in afterwards. Do feel free, each of you, to comment on the answers, if you so wish.

This question is very general. What is your view on the Bill? To what extent do you think it is necessary, and how will it improve and affect the operational work of your respective organisations? Do you feel it goes far enough?

> ***Michael Atkinson***: Thank you, Lord Chairman, for inviting us here today. We are pleased that yesterday was of benefit, hopefully to you all, to see how our working practices take place.
>
> Could I first introduce us? My name is Michael Atkinson. I am the secretary for the National Police Council's Data Communications Group, and I work for ACC Richard Berry, who appeared in front of you several weeks ago. To my right is Detective Superintendent Matthew Long. Matthew is a deputy head of UK operations within CEOP, which is part of the NCA. I hope that Matthew and I may be able to provide you with some evidence on our use of CD and how this relates to the Bill. On my left is Detective Superintendent Paul Hudson. Paul leads and is the head of the Metropolitan Police

Service's technical surveillance unit. He will, I hope, deal with any questions you have in relation to equipment interference.

The Chairman: Thank you very much indeed. Of course, we met some of you yesterday. Anyway, what is your view of the Bill? Is it right? Is it necessary? Does it do what you want it to do, and does it go far enough for you?

Michael Atkinson: I suppose it is no good me sitting here talking to you about the change in technology. You have probably all seen enough, since you have been in this Committee, about how technology has changed. What is happening with policing? We are struggling. How are we struggling? We are struggling to keep pace with how victims, witnesses and criminals use technology. In many investigations, we try to use CD as evidence. It is causing us problems to obtain this evidence. We use CD in many investigations: theft, child sexual exploitation, homicides or frauds—a wide spectrum of offences. Our inability to obtain this data is increasing, for various reasons. Some CSPs do not retain the data for long enough in certain services. Some CSPs are outside our jurisdiction; we have difficulty with their laws in obtaining the data, and some CSPs outside our jurisdiction will not assist us. Also, some of the data is not retained. I have said that it is not retained for long enough, but the actual data that we require is not retained. We believe that this Bill will assist in closing some, but not all, of the gap that we are currently experiencing.

Paul Hudson: Lord Chairman, if I may I will also bring you the EI perspective on this. We would seek further capability. The Bill currently provides extra oversight, which we welcome, but it is all about serious crime. On very rare occasions, as I hope we demonstrated yesterday, we might use EI to protect the most vulnerable people, and that might not be in serious crime; it might be to save them from doing harm to themselves. So, in the emergency provision, we would look for something that legitimises that use of EI: to protect the most vulnerable people from harm.

Q163 Mr Hanson: Thanks for coming in. My apologies for yesterday; I was on another Select Committee elsewhere in the building. For my benefit, but also to put it on the record, it would be really useful if you could give a couple of concrete examples of how the current use of powers has led to convictions or, as you have said, has been of help in providing safety or rescue to individuals.

Michael Atkinson: Unfortunately, you were not there yesterday, because you would have been provided with evidence that clearly showed how we use communications data in protecting the vulnerable. You would have seen and had explained various examples of young missing children and people who were going to commit suicide. Unfortunately, we did not manage to save everybody.

We use the vast majority of communications data to protect the vulnerable and save people's lives. In addition to that, our use is predominantly in two areas of our business: proactive and reactive investigations. That is what we use communications data for. In proactive investigations, we may use it to identify a conspiracy and people talking to each other. We may use it to identify people's whereabouts at certain times. We also use it to identify other leads; for example, somebody may have phoned a travel agent and it gives us a lead so that we can go there. We may be able to get that information, take further steps and make further inquiries. So in proactive investigations, we use it in various ways.

In reactive investigations, the offence has predominantly taken place. Murder is probably one of the more serious crimes that we look at. My background is as an SIO, and in every murder investigation in which I have been involved we have used communications data. Why do we use it? We need to identify where the victim was and where their last movements were. It may be over a 24-hour period or it may be just a relevant period of time. We also look at and identify people with whom they have had contact and, again, that may be over a 24-hour period or a specific time period. That is no different when we identify a suspect: we would look at their data, their locations and who they are talking to. We use it across various offences.

We use data together with forensics and other data opportunities, such as ANPR and CCTV. In 2012, we undertook some work and identified communications data use in 95% of all serious crime prosecutions. We use communications data in 100% of counterterrorist investigations. Matt will probably give you some more examples of how it is used in CEOP and its work.

Matt Long: In answer to your question, the Bill is essential and invaluable. I will give you two operational examples. First, the National Crime Agency's CEOP receives between 1,300 and 1,500 referrals every month from the National Center for Missing & Exploited Children in the US, the majority of which are reported online. Every one of those is a child at risk or a suspect for us to identify, and with the majority the starting point is the communications data. For each of those, myriad further victims or suspects may be identified who we need to follow, so in the daily, weekly and monthly movement in the National Crime Agency that is the volume that we need communication data to support.

A more personal example is that I am still the senior investigating officer for Operation Notarise. Within that operation, we arrested 745 offenders nationally. Every single one of those offenders who we arrested had a comms data application attached to them, and some had multiple applications. Within that investigation, we safeguarded over 518 children, so as the senior investigating officer I see it as a tool in the toolbox, although not the only tool; it is complemented by other tools such as open source. To summarise, there is that daily, weekly protection of children. In the large-scale and small-scale operations, we need it critically to progress.

Mr Hanson: What areas of new media are you not able to access now because of the way in which the legislation is currently framed?

Matt Long: A very simple example, which I was going to come on to later but will bring in now, because it illustrates it, is in grooming. With the grooming of a child on a communications platform that is online only, if we request that data we want to know who that child is talking to. Who is that offender? Are they talking to other offenders or children? There is some data that we simply cannot get. If that is the only route by which they are communicating, which is increasingly the case, it simply is not available to us.

Mr Hanson: What is the difference between seizing PCs and seizing mobile telephones to get that data, as opposed to having the powers under this Bill?

Matt Long: You need to have the computer or the phone to be able to do it in the first place. Our difficulty is that we may have a report that has come across from the National Center for Missing & Exploited Children, which says that a child is in communication

with an individual, and we do not know where they are and do not have the devices. It is quite easy once you have the offender in custody and you can go to the device. Then we will proportionally assess those devices and see how many offenders we can identify and other routes that we can follow. Ultimately, sometimes the very first step is that communications data. Without it, we cannot take the first step, which is the identification.

Q164 Lord Strasburger: Good afternoon, gentlemen. Is accessing internet connection records, if that can be done, essential for the purposes of IP address resolution and identifying persons of interest?

Michael Atkinson: I have spent several hours in one of the UK CSPs for mobile phones. I cannot sit here and say that I am a technical person who understands the technical issues to do with how telephones are used, how they retain the data, what data they retain and what they might need to do to provide ICRs. What I can say is that they are assuring me that, without the retention of ICRs, they will not be able to solve internet protocol resolutions. They also tell me that we will not get the evidence that we need in order to undertake further investigations of people who may be of interest to us. Matt has given you one example. Another example is a terrorist investigation. We do not do live inception in all terrorist investigations that we undertake. We may do investigations for months and months, identifying intelligence, connections between people and what the suspects are intending to do. If we are investigating some suspects and have some intelligence but it is insufficient to arrest, we would like to know whether they have gone to a website on how to make a bomb, whether they have gone to a website of a major shopping place in the UK, whether they have gone to a website where they might wish to book some tickets to leave the country. Currently, we cannot get that. We believe, and we are told by the communication service providers, that ICR will solve this.

Q165 Shabana Mahmood: Last week we had oral evidence from a number of smaller CSPs, and one of the things they said on internet connection records that struck me as important was that the internet connection record would probably provide a useless bit of information. If you had a mobile telephone for a young missing child, for example, all the ICR could tell you is that that phone had been connected to Twitter or Facebook for 24 hours a day for the last six months from the point at which the phone was bought, because many of the apps that are used are automatically connected to the internet. I have just checked my phone. I have background app refresh on, which means that it is automatically connected on a 24-hour basis. Is there a danger that lots of information that you collect from internet connection records is just useless: it gives you no additional investigative assistance?

Michael Atkinson: Again, we look at what we are being told by the largest CSPs. If we have a missing person, we conduct a lot of inquiries. CD may not be our first inquiry. We have other inquiries to undertake, but we may identify that the missing person has a phone. What better way to trace them than through the cell site to identify where they are?

Sometimes phones have been turned off, but we can get back the fact that they have been talking on Twitter to somebody. Even just by getting that back, we can go to Twitter. Twitter, and not necessarily just that company but other companies, will help us to identify vulnerable missing people. They will identify to us that they may have been in contact with certain people, who would give us further lines of inquiry and may allow us to identify where this missing person is. ICR could tell us that they have booked a train ticket. They have gone to a train line; it looks as though they have booked a train ticket.

We can make inquiries with them. We can see that they have. Maybe we can locate where they have gone. The CSPs that I have spoken to have made it clear that ICRs would assist us.

Shabana Mahmood: National Rail Enquiries, which is the main app that most people use for booking their train ticket, is on 24-hour background app refresh. I suppose this Bill is introducing a whole new regime for internet connection records. My question is: is it necessary? Will it just give you oodles and oodles of useless information? If you are trying to trace a child, you know they are on Twitter and you can get into their Twitter account or ask their friends, who are more likely to be able to tell you what the Twitter or Facebook activity of that young person was.

Michael Atkinson: That is what we try to do, but there is always this issue. Matthew explained the relationship with grooming. We can get a lot of information that can assist us to identify where they are. We realise that there is collateral intrusion. We realise that there are risks to this, but on the other hand there are children and missing people. Are we willing to go further to try to save a life or to bring the person back to their family?

Stuart C McDonald: First of all, just following up on those points, in quite a lot of missing persons cases, for example, it must be pretty straightforward to establish whether the missing person has a Twitter or Facebook account and then, once you have done that, you can go to these communications service providers and find information about who they have been contacting and so on.

Michael Atkinson: Sometimes we can, yes.

Stuart C McDonald: How often are you frustrated in trying to find what people have been doing to communicate with others?

Michael Atkinson: I cannot sit here and say how often it happens. What I can say is that it does happen. Some companies will not assist us; some companies that are outside our jurisdiction will not support us and help us with identification, but many of them do.

Q166 Stuart C McDonald: Now, as you will understand, the proposal is for communication service providers to be required to retain communications data and internet connection records for 12 months. What is your comment on 12 months being the specific limit? Would you want more than that, or could you cope with six months or three months?

Michael Atkinson: It is interesting that this has come up several times. I was involved in the 2012 Bill. In 2012, we undertook a survey across policing. Sixty-four law enforcement organisations, in 2012, undertook applications for communications data. We received replies from 63 organisations. They undertook a two-week survey in every SPOC unit. The unit that you went into yesterday recorded, over a two-week period, every application that went through the unit in each of the 63 organisations. That gave us a really good breakdown of how we use communications data, but also of the history of the data that we are applying for. To give you an example, we covered nearly 10,000 pieces of data and applications. That is what this survey was about. Nine per cent of those applications were for sexual offences. What was interesting was that 37% of that 9% of data that we applied for was more than six months old. We would say, and you can see, that retaining the data for more than six months is very important. We also identified that 1% of all the data was

for terrorist investigations, and 27% of that data was more than six months old. Now, I know we are writing to you, Lord Chairman, and we would be happy to provide that data to you with our submission, but it provided us with some really good background and understanding of why. Further, it shows what is more than nine months old or 12 months old, so there is more data there.

What is really interesting is a document produced by IOCCO on 20 November, only last month, which is a breakdown of communications data and applications. It shows over 100,000 communications data applications, 19% of which were in relation to sexual offences. Two things jumped straight out at me. First, this is a 100% increase from the survey that we did in 2012. Secondly, 37% of roughly 19,000 is over 7,000. We would say that, if we retain data for only six months, hundreds if not thousands of suspects for sexual offences would likely evade prosecution.

Stuart C McDonald: Can I just pick you up on that, though? That information is very useful, but it does not tell us how crucial that information is at six months old, 12 months old or whatever it is. I suspect it is almost impossible to gather that, but what is your personal view?

Michael Atkinson: We have had the conversation about when we undertake investigations. A homicide investigation is a bit like a jigsaw, but you need all the pieces to make the picture. I will have communications data. I may have CCTV. I may have forensic data. I may have ANPR. There are quite a few pieces to make up that jigsaw. What you cannot necessarily say is which piece was crucial in detecting and prosecuting that person for that offence. The whole picture helps to prosecute, not an individual piece.

Q167 Victoria Atkins: Following on from that, perhaps this is an easier way of looking at it. Is there a single serious organisation case that you have investigated and taken to trial in the last decade that has not involved mobile phone records or records of telephone communications?

Michael Atkinson: I cannot sit here, hand on heart, and say 100% that there is, but the data shows that in 2012 we used it for 95% of all serious and organised crimes. I would be very surprised if any serious and organised crime case went to court where we had not used communications data.

Matt Long: Perhaps I could elaborate further for you. I gave the example earlier of Operation Notarise, with 745 arrests and 518 children safeguarded. In that operation, within a 12-month period, we resolved 92% of data. If I had 12 months, I would get a 92% return. If that dropped to six months, I would lose six out of 10 of the pieces of data. Out of six months, we would lose 60% of that offending population. If you dropped it by a further 12 weeks, I would have lost 87% of the lines of inquiry presented to me. In that case, the first point was communication data. To answer your question about what the impact would have been on me in that operation, it would have been those percentages at those time stamps. When you think about that in relation to that operation, the majority of the offenders in that operation were not known to law enforcement. It is not as though I have another database that I can check and then identify that person by some other means. I simply cannot do that. When you think that 15% of those people were in a position of trust—they were a teacher, a scoutmaster or in another position where they were the guardians of our children—it is very unlikely that I will find another route, because those individuals have gone through criminal record checks. They have gone through the very

good safeguards that we have as a country, but effectively they have beaten them. That example shows you what the output and the outcome would be if you reduced the length of retention in those ways.

Michael Atkinson: Sorry, Lord Chairman, could I just cover one other point? We do not use communications data just to prosecute people. We clearly use it also to prove that people have not committed an offence. The defence uses communications data. For our more serious cases, especially if we are talking about counterterrorism, homicides and serious and organised crime, can take six months, nine months or over a year to come to trial. If the defence serves their defence statement on us six or seven months after the offence has taken place and we only retain data for six months, it would prevent them from having a fair trial and it would prevent us from checking alibis and defence statements, so we believe that 12 months is the appropriate period.

Matt Long: Can I make one final point on that? The other thing, going back to your point, is that victims do not disclose on day one when the communications data is available to us. It may take them weeks or months to gain the confidence to disclose. Then, we do not get a consequential order of victims so that we know that A leads to B who leads to C. It might be that A leads to E, E leads to another 100, and we have to review them. All that takes time. It is not necessarily even at that first instance of the offence when we need the data. We need to conduct the investigation and be allowed sufficient time to do that. Sometimes that can take months.

Q168 Dr Andrew Murrison: Good afternoon, gentlemen. Twenty years ago, we did not have any of this technology available to us, so setting aside crimes that are specific to modern communications such as online paedophilia et cetera, it follows from what you have said that since you now do have access to all these investigative modalities, your clear-up rate should have been dramatically improved and your ability to secure missing people, for example, should have been improved. Is that in fact the case?

Paul Hudson: As much as we have greater technological investigative powers, the criminals we seek to arrest and bring before the courts also have greater technological ability to avoid us. We have seen that the increase in technology, the mobile nature of communication and the mobile nature of making meetings have made it more difficult. The criminal of 20 years ago used to meet at a safe house and it was a lot easier to understand how they communicated. The criminal of today tends not to do that, because they have the ability, as we all do, to communicate on the move. Our capability is merely moving with the capability of the criminals we seek to address.

Q169 Dr Andrew Murrison: I am not entirely satisfied by that, since you do have an increased range of ways in which you can keep tabs on criminals and investigate them, which draws me to my next point, which is on equipment interference. My first question is: in what proportion of the cases that you deal with is equipment interference used?

Paul Hudson: I do not have the percentage proportion.

Dr Andrew Murrison: What is the ballpark figure?

Paul Hudson: It would be the majority, but it would be difficult to answer in a public forum.

Dr Andrew Murrison: It is a majority of the serious crime.

Paul Hudson: It would be difficult to answer in a public forum.

Dr Andrew Murrison: That is interesting. Okay, perhaps we can come back to that. What concern do you have about the evidential nature of the material that you can generate using equipment interference? In other words, can it be admissible in court, and is it degraded in any way and thus rendered inadmissible?

Paul Hudson: The whole point of law enforcement is to gather evidence that we can place before a court—the best possible evidence. Everything we do is aimed at that. It is covert by nature, but we would not do anything that would degrade that, because when we come to trial we would have to place before the court evidence that we can adduce and provide a fair trial. Nothing we do would reduce the quality of the evidence that we are collecting.

Dr Andrew Murrison: Are you at all concerned that what you do by way of equipment interference poses a risk to wider users? Clearly what you are doing has been characterised as being legalised hacking. I know that is an awful generalisation, a bit like the snooper's charter, and we should really bin those kinds of clichés. Nevertheless, it is the way the *Daily Mail* would present it, for example. That suggests a certain amount of damage that is being done or caused—damage that, since it is associated with the state, is potentially the subject of some sort of comeback against the agencies. Have you any cases where that has happened? I suspect you would not be very happy to share them in a public forum. Are you at all worried that your capability to do this work will at some point come back and bite us?

Paul Hudson: First, I am not. Equipment interference is a covert capability, so nothing that we do under equipment interference would cause any damage or leave any trace, otherwise it would not remain covert for very long. Again, the endgame is to collect evidence to place before a court. If we were causing damage to equipment, that would reduce the ability for the evidence to be alluded to.

Dr Andrew Murrison: You are confident that your activities, by way of equipment interference, will not in particular harm innocent people and render innocent systems compromised or inoperable.

Paul Hudson: Before any deployment, a risk assessment is conducted, and that is part of the authorisation process that would be reviewed by the authorising officer. Subsequently, before authorisation is given, all those risks would be outlined for the judge or the judicial commissioners. Of course that would affect the proportionality and the collateral intrusion that would occur.

Michael Atkinson: I want to cover one thing that Paul said about the majority. We will provide some data, if required, on the use of this type of equipment. We would ask that it is not shared in relation to any reports, because it is very confidential. The other point is that I think it was quite clear, in a couple of the investigations that were shown yesterday, how important this is to us. I will not go into any more details about that.

Matt Long: On the change in crime that we have seen recently, we are starting to see victimless prosecutions, where we have the video of the rape of the child, who is a neonate, too young to talk, but we have the opportunity to use comms data to identify that

and to recover that evidence. For CSE, there are very specific examples where the child is unable to report and we use that data to bring a prosecution, which we would not have been able to by any other means. The conviction data, which I am sure can be provided if requested, shows a year-on-year increase in the responsiveness of the UK to deal earlier with indecent imagery of children across the country. In my particular area, there is a very definitive use that can be seen.

Lord Strasburger: On the evidential quality that comes from computers that have been subject to equipment interference, the other risk is that a guilty person could get off if his defence lawyer discovers that equipment interference has taken place and alleges, for example, that material was planted on the computer at that time. I can see a risk here, and I think others can too, to successful prosecution using evidence from that computer if a third party—in this case you—has had their fingers in it.

Paul Hudson: As we discussed yesterday, equipment interference does not stand alone. As already described, an investigation is a jigsaw puzzle of evidence that is placed before the court, and we would use the current judicial process under the CPIA to ensure that the judge in PII was made fully aware. We would obviously reveal all to the CPS, which would then, through the prosecution counsel, place it before the court and the judge to ensure that the judge knew exactly what had happened, how we did it and our methodology, so that he or she could take a decision on fairness. We would merely place before the court the evidence that is adduced. It would be for the judge to decide.

Q170 Lord Strasburger: Thank you. Can I just talk briefly about intercept as evidence? The lawyers in the Home Office have various views on the admissibility of intercept as evidence. It would be very interesting to hear from policemen at the coalface how helpful or not that would be for you.

Michael Atkinson: We are aware of many studies. It is not our part of the business, although we understand it and know it takes place. It is up to the people who are involved in that area of the business to decide whether they feel it should be used as evidence, and not us.

Q171 Suella Fernandes: Good afternoon. Could you describe for us the oversight and monitoring regime that regulates the process?

Paul Hudson: The majority of the current regime is under the property Act. Originally, the applicant will make an application and lay out their view on proportionality and necessity, as defined, and justification. Under the Bill that is reviewed by a chief officer, who will make a similar assessment. Then it is passed to the judicial commissioner to review and authorise. My understanding is that that is independent, which is welcome. The Act makes it a lot clearer that we have this ability to use it and that we would use it. It is more foreseeable in line with David Anderson's recommendations. Under the Police (Property) Act 1997, the intrusiveness depends on the level of intrusion by the surveillance commissioners. The less intrusive methodologies that we use are authorised and then reviewed, and for the more intrusive methodologies we have to get prior approval under the IP Bill, which is good. We welcome that.

Outside that, my understanding is that the Bill is going to bring together the three different oversight bodies, IOCCO, the OSC and the Security Committee, and make them one. They

will continue in that yearly review and that regular inspection of our capability, in line with how it works today. The two different commissioners for the police come to us, look at all our records, look at how we have deployed, what we have deployed against and have free run of all our databases. It is a much more stringent oversight for us. It is clearer and better in relation to my part of the business.

Suella Fernandes: What practical impact do you think the proposals will have on the process of getting permission to use the powers?

Paul Hudson: Personally, providing there are enough commissioners and the speed is available, there will be no real impact, and the emergency criteria also fit. As I said, it reflects the police Act, so I do not feel that there would be a lot of change.

Michael Atkinson: For CD, we would say that the oversight probably begins at the point when the SPOC becomes involved. Yesterday you heard about the role of the SPOC, and how important it is as a gatekeeper and for the advice it gives.

Suella Fernandes: Sorry to stop you there, but is the SPOC an independent person?

Michael Atkinson: They are independent of the investigation. They have a specific role within the organisation just to apply for communications data. They have first oversight of an application, and then it goes to an independent authorising officer. If it is for subscriber information, it is authorised by an inspector who again is trained and has to go through the full process to understand the application and justify whether it is proportionate and necessary. For anything else, it is a superintendent. Again, he is trained. He understands all the issues involved in making an application.

In addition, clearly we have the IOCCO inspections. These are now undertaken yearly with every force. They interview staff. They obtain some of the applications that we have submitted and review them. They may speak to the investigating officer in order to understand whether the application was submitted correctly. We consider their inspections to be challenging and robust, and we fully support them. They provide us, at times, with advice and guidance in their reports on forces. This can assist with our training. We look at the advice and guidance. We have tradecraft events throughout the year for SPOCs, SPOC managers and DPs, and we ensure that if errors and issues are identified in their reports on policing, we discuss them and look at training to improve what we are doing. We would say that the oversight is good. If the oversight was the same under the new justice commissioner, we would have no issues with that.

Q172 Matt Warman: Just following on from that, what consideration do you give to protecting innocent individuals from the impact when you are investigating people who you obviously have suspicions about? There would be some collateral damage, if you like.

Michael Atkinson: There is clearly an intrusion into somebody's private life whenever we apply for communications data, and throughout the process everybody understands that. We take access to this data very seriously. Again, you heard yesterday about the process and that the initial applicant may be a PC in a station who decides that he is dealing with a theft and the only contact that the victim had was over the phone. They may wish to, and probably will, apply for subscriber details for the person with that phone. That applicant, when he submits that document, will look at necessity and proportionality and whether the

application is justified. I cannot sit here and say that they would definitely look at collateral intrusion, but I would say that when it gets to the SPOC the SPOC will definitely look at collateral intrusion. It is the same for the DP, who will definitely look at collateral intrusion, necessity and proportionality. The gatekeepers of the SPOC will know whether we can even get this data, because it is no good putting in an application if the CSP will not even provide the data, but it happens, probably because people do not understand that some providers will not give us the data.

We have a failure rate and a refusal rate, which shows that we treat this as serious and as an intrusion into people's lives. This varies across forces, but it shows that we can refuse applications because the data is not be there but the SPOC may identify in the very early stages that it is not justified, proportionate and necessary. That can happen at that stage. The next stage is going to the DP. The DP can refuse applications. As a DP I have refused many applications. There are other courses of action that people could take. The role of a DP is not taken lightly. You understand that you are interfering with somebody's private life. I would say that the process that we have deals with those issues.

Matt Warman: Finally, once you have all this data yourselves, once it has been obtained, how do you make sure internally that that data is not vulnerable to being accessed inappropriately, either by your own people or hacked by the outside world?

Michael Atkinson: All SPOCs have PINs so that only they can access the data, which is in stores and in police organisations. Mr Bristow mentioned that no store is definitely safe, but these stores are not the same stores that our other database is on for outside access. People have to have a password to get into it. If we felt that anybody had got into this, we could go back and search who had entered, so I would say that they are very secure.

Suella Fernandes: I have a follow-up question. You talked about the test of necessity and proportionality. What factors are taken into account when you are ascertaining whether this is necessary action and is proportionate?

Michael Atkinson: For a lot of investigations, the first thing I consider is the offence. If I have a murder and I have a victim or a suspect, is it necessary? Of course it is necessary; we need to identify where that person may have been in the last 24 hours or the last two hours. Is it necessary that I need to identify who they had contact with? Yes, of course it is. That is how we conduct the investigation. Alternatively, it could be, as I have had a couple of times, somebody who had given their address over the internet or over the phone. This was several years ago, when fixed-line internet connection records—IPAR—were easier to solve. Somebody would give their address, but the first thing they were applying for was communications data. Was it necessary? You have the suspect's address. Was it proportionate? It was definitely not. Was it justified? No, you have the suspect's address; go and knock on the door. When we make these applications we take into account the offence that we are investigating and the collateral intrusion. Do I need the data for 12 hours when I am looking for my victim in an hour's period? We take all this into consideration, and that is why the process is robust and works well.

Q173 Lord Butler of Brockwell: Some of us were shocked by the use of communications data in the plebgate affair. Do you consider that use of communications data proportionate to the offence that was being examined?

Michael Atkinson: I have not been involved in the plebgate affair. I am not a Metropolitan Police officer. Without my knowing the full knowledge of the offences, what was being investigated, the level of intrusion and what they were applying for, I cannot answer that. I would need to know more information.

The Chairman: Thank you all very much for a very useful, very informative session. Thank you so much for coming along.

Witnesses***:*** **Rt Hon David Davis MP** and **Baroness Jones of Moulsecoomb**

Q174 The Chairman: Mr Davis, Baroness Jones, we are very grateful for your coming along to the Committee. We think that you have some very interesting things to say about this Bill, and I will kick off by asking a question that is so general you can make a general statement before individual questions. The same question, first, perhaps to Mr Davis and then to Baroness Jones: is this Bill necessary, and to what extent does it address your concerns, if it does so at all, about legislation in this area?

David Davis: Thank you for the welcome, Mr Chairman. It was either you or the Berlin Christmas market. You won this time, so I have just leapt off a plane. Is it necessary? Yes, it is necessary. There is no doubt that we need a new Bill. It is taking over, if you take David Anderson's count, something like 66 statutory mechanisms for various forms of interception, data gathering and so on, many of them based on bad laws. RIPA is a bad law. I am sure some of your witnesses have told you that already, but it is very badly drafted. I can come back to that in a minute. It is also taking over laws that are used in ways that I am quite sure Parliament did not intend.

I would have hoped that it would have consolidated all the electronic surveillance laws into one area. It has not done that, so its first failing is that it has not concluded that. You have just had witnesses from law enforcement agencies, have you not? The police Act is still effective. IMSI-catchers, the devices that block and intercept mobile phones, for example, would go around this, and that is part of the propensity to expand on the part of the agencies. All agencies in the world expand their powers, and this encourages it.

It is good for another reason and that is, in a consolidated form, that it will be possible not to future-proof it but to future-adapt it. A lot of the argument that you get from the agencies is that we have to make this future-proof, which tends to be an argument for making things more general, open and loose. That is a bad idea, but we are probably going to have to get into the habit of probably having one of these Acts every Parliament anyway—just as we have a Finance Act every year and a Companies Act every year or two—because of the rate of change of technology.

Does it meet all my concerns? You would be surprised if I said yes, would you not? The answer is no. On authorisation, which again I am sure we will come back to, it is a missed opportunity, because a new consensus was developing on judicial authorisation. They have missed that. It is certainly not what somebody described as world-leading. If I had to pick the world-leading country in this area, I would probably pick the United States for where it is arriving at now rather than us. I do not think that the double lock is very good. It claims to introduce one new power, but in practice you have internet connection records as well as effective recognition or avowal of bulk equipment interference, bulk personal data sets, bulk data and even thematic warrants. Although they were not formally approved by

Parliament, somehow they were invented out of RIPA. There are a whole series of areas where it is weak, but broadly speaking we have to have a Bill along these lines.

The Chairman: Baroness Jones, if I can just repeat the question, is the Bill necessary, and to what extent does it address any concerns you might have about legislation in this area?

Baroness Jones of Moulsecoomb: Lord Chairman, thank you very much. I am missing our team Christmas do and they are all in the pub waiting for me, so I am sure you will understand if I speak quickly. I suppose you could say it is necessary, because times are moving on. Obviously we now have huge ability in surveillance, and so some sort of way of containing it and monitoring it is incredibly important. The majority of powers in here are new.

My concern is twofold. First, this is covering what has been done up to now, because the laws that have existed so far have been broken and abused many times by security agencies and by the Met. I have quite a list, which perhaps I could give you subsequently. I am concerned that there is a good operational case for this and that they really understand how to use the powers. I am concerned that they are going to use these powers to spy on people who are holding them to account, because this is what has happened already. Security agencies and the Met Police have used powers that they do not have to spy on people, for example Doreen Lawrence, who tried to hold the police to account. Mark Thomas, who is a comedian, tries to hold the state to account. There are five journalists who have been spied on so far, and even I had for 10 years, when I was an elected person sitting on a police authority, a file on me in the Met's domestic extremist database, which is fairly outrageous. I am quite clear; my life is quite public and there was nothing to hide, so I do not feel that I was intruded upon, but at the same time what a terrible waste of time and resources, and it was not just unnecessary but unlawful at that stage.

There is also the fact that Snowden has told us that GCHQ intercepts 50 billion internet communications a day. Now, that is an astonishing amount of data coming in. Over the years, I have asked the Met Police how many databases they have to get an idea of how much information is coming in. They could not tell me to the nearest hundred or to the nearest thousand how many databases they had, so we are looking at something that is potentially very complicated. There is a vast amount of information coming in. Do they have the skills to deal with it?

Q175 Suella Fernandes: I have one general question. Do you agree that the Bill before us today represents progress compared with the Draft Communications Data Bill in 2012?

Baroness Jones of Moulsecoomb: I would say that there are things in here that I am deeply unhappy about.

Suella Fernandes: How does that compare with what we last saw in 2012, in that now local authorities do not have any powers? That is a movement from 2012, is it not?

David Davis: There are marginal improvements. There is no doubt about that. As I said, the fact that there is a single Bill of itself is an improvement, but it is a long way short of what it should be. One of the things that worries me, Chairman, and I hope you will take this in the spirit it is intended, is that it is going to be incredibly difficult for you as a

Committee to deal with this Bill in the time available. It is an enormous Bill, particularly when you take on board all the newly avowed powers. They are not new powers in the sense of being used, but they are new for Parliament. Assessing whether they are right or wrong, effective or ineffective and proportionate or not an erosion of privacy is going to be incredibly difficult, and in this business speed is the enemy of wisdom, so it is quite difficult.

My comment is that they are granny footsteps towards a better position. We must not miss the opportunity to get this right, both from the point of view of protecting the values that we are supposed to protect and, on the other hand, making the agencies more effective. They are behaving in a very different way from some of our allies, who are arguably more effective.

Baroness Jones of Moulsecoomb: The Government appeared to make some concessions, because there was quite a furore about this. For example, they brought in judicial review, but the judicial review is very light and in fact can be completely ignored. If Ministers decide there is some sense of urgency, they can go around the judges altogether, despite the fact that the Royal Courts of Justice has a judge on duty 24 hours a day. They appeared as concessions but they do not go far enough.

Q176 Lord Butler of Brockwell: If I may follow up that point, when you say that the Government could ignore the judges completely, are you referring to it being within five days if it is a matter of urgency?

Baroness Jones of Moulsecoomb: Yes.

Lord Butler of Brockwell: If I may respectfully say so, surely that is not ignoring the judges completely.

Baroness Jones of Moulsecoomb: They can bypass them.

Lord Butler of Brockwell: It is for five days.

Baroness Jones of Moulsecoomb: Perhaps I can talk about the volume of stuff that is coming in. The Prime Minister will be told if there is a warrant for people like us, for example—privileged people. For me, those are the people we are going to have to be very concerned about. These are the people who get whistleblowers coming to them, whether journalists, ministers of religion, parliamentarians or whoever. The Prime Minister will be notified of a warrant but does not necessarily have the right to reject that. The warrant will go to a judge. Am I saying this wrong? The judge or the commissioner only reviews it. The judge is not able to say yes or no. The Minister can then take it to the investigatory powers commissioner, who can overrule the initial commissioner, so there are lots of ways in which these things can be pushed through.

Lord Butler of Brockwell: I will not continue this, but the investigatory powers commissioner is of course a judge.

Baroness Jones of Moulsecoomb: Yes.

David Davis: Lord Butler, can I give you my view of this, which is not the same? I do not view the accelerated procedure as a necessary bypass. It is going to have to be refined in some ways, but of course there are circumstances in which fast decisions have to be made. In the London/Glasgow bombings, for example, telephone data was very important and you had to make a decision very quickly indeed—maybe in minutes. You have to have a procedure like that. There is of course, in my view, a need to keep a very close eye on it and maybe publish how many times that is triggered every year. Frankly, make it plain to an officer who uses that procedure that if he is in the wrong there will be a mandatory warning on his record, but I do not see it as a bypass. I do not share that concern.

Q177 Lord Butler of Brockwell: Thank you very much. Could I get on to bulk interception? Are you satisfied, and I may ask each of you in turn, that the operational case has been made for bulk interception, bulk acquisition of the collection of communications data and bulk equipment interference? Perhaps I could use my second bit of ammunition before I ask you this question. This is a matter that David Anderson looked at and said he was satisfied that those powers were necessary. Do you agree with him?

David Davis: I do not entirely. Let us take bulk interception first. It is insufficiently narrowly defined for foreign for example. Charles Farr, when he gave evidence in 2012, I think, said that the selectors on the bulk intercept data would obviously pick up British-to-foreign intercepts and would treat accessing Facebook, Twitter or any foreign platform as appropriate for this. That seems to me to be too broad and that they have not made the case to justify it being that broad. If we are talking about bulk intercept of a fibre optic going through Cyprus to Pakistan, I am going to be more relaxed about it. That is the first thing.

Your second point was about the bulk acquisition of communications data. The best model here is America's. They basically recoiled from that after the President's panel had a really deep look at it. There was a previous director of national intelligence and very serious counterterrorism lawyers on the panel. They looked at it and came to the conclusion that what they were doing was simply not worth it. We would have to make a much stronger case to come back on that.

On bulk equipment interference, individual targeted equipment interference is obviously a necessity, particularly in this day of encryption. It is one way of getting around encryption and probably the most effective, but bulk interference worries me a lot. It is a very serious intrusion of everybody's privacy. We know already that one of the agencies has effectively suborned very large numbers of SIM cards—in the millions. That sort of thing worries me. Apart from the direct assault on individuals' privacy by the state, it would undermine the integrity of their own personal security to anybody else—to a blackmailer or to somebody trying to intercept them.

One group that you did not mention which I am going to raise because it almost falls off the tongue is bulk personal data sets. It is avowed, but there is very little in here. It is not for me to give the Committee advice, but if I was going to point at something that needs to be looked at, I would look very hard at that as well. This has explicitly been disavowed as an approach by the Americans and others, and it really is completely antagonistic to the things that the current Government and the previous Government set their face against. In the identity card arguments, the primary argument about the identity card was not about carrying a plastic card but about the existence of a central national database of personal

data on every citizen, and it sounds to me as though we have had that since certainly 2005 and possibly 2001, which is what shocked Mr Clegg. There is a very large number of areas where other people have found that these are very bad ideas and do not work and have recoiled from them, sometimes even the agencies without external intervention, on cost-effectiveness grounds. We need to have a much tougher, more challenging attack on this if we are going to justify it.

Lord Butler of Brockwell: Just on that last point about bulk personal data, are you reassured by the fact that under the Bill this would now require a warrant that would have to be endorsed by a judge?

David Davis: That is an improvement, but on the very holding of this, I do not know whether you can see the data sets that they have. We are pretty sure, at least reporting on the register today, that they have all the communications data. They have flight data. They almost certainly gave financial data. They may well have ANPR data. This is very intrusive information for a state to hold. We have been having arguments for the last 10 years about whether we should have a central database for ID cards, or whether we should have communications data, hence the stalling of the so-called snooper's charter, when in fact this has existed throughout that. One thing that I would hope the Committee would come to a view on is what is in this, because there are arguments that there are hundreds of data sets here per person, which is really very serious. Yes, you are right that warranting is good, but frankly the extent to which much of this database should exist is very debateable.

Baroness Jones of Moulsecoomb: There are also, of course, medical records and financial asset records, and so on, in those data sets. It is a very wide scope.

Lord Butler of Brockwell: Baroness Jones, do you want to add anything on bulk collection?

Baroness Jones of Moulsecoomb: The bulk collection of domestic phone records, of course, has been proved to be ineffective in the States under a similar power. The President's review group said that it was not essential to preventing attacks. The Privacy and Civil Liberties Oversight Board concluded that it had not identified a single instance involving a threat to the United States from that sort of collection, so I would argue that it is of very limited value.

Q178 Victoria Atkins: Just on that point, you have listed all sorts of information. What is the basis for asserting that those are sets of information held by the authorities? How do you know? You have told us that with some confidence.

David Davis: Some of it has been around. The place to look is an organisation that used to be called GTAC—probably in your day, Chairman. It is now NTAC, the National Technical Assistance Centre, based at Thames House. It has already been recognised in public by Ministers that intercept data is there. These are the people who handle most of the requests from all the agencies. It has been in the public domain that there is a financial set, which I assume is credit cards and bank records, because GCHQ has a title for it: FININT. Flights we know about. The question was about the rest. As to whether or not they have ANPR, it would be very surprising if they have this and have not put ANPR in it, for example. If I were going to build a database like this, given their purpose, that is what I would do. It needs to be answered. One of the things that has been said for a start

by a number of security journalists, who know their way around this, is that they think there are hundreds of data sets—not one, not five.

Victoria Atkins: Do you worry, in listing these data sets as you just have, that you have given some very helpful information to serious organised crime gangs, terrorists and others?

David Davis: In that case, I would arrest Malcolm Rifkind, because he drew it to the public record in March last year. It was only when that was done that this was put under the intelligence commissioner's oversight. Until then, there was no oversight whatever. I am afraid that in a democracy it is necessary to look at what you are doing, and you can only do that by discussing it.

Baroness Jones of Moulsecoomb: The scope very definitely has to be well defined, which it is not at the moment. There is also the fact that once you have warrants for this bulk information, access is much freer. Once you have it, there are stacks of stuff in there that you can freely search whenever you have an appropriate moment. It is not just a one-off search.

Victoria Atkins: I have a question to both of you: what is the correct balance between the democratic accountability of Ministers and the independent oversight of judges in the authorisation of warrants? Does the draft Bill get this right?

Baroness Jones of Moulsecoomb: I would like to have seen a little more of the judges being able to look at the legal aspects of whether or not to grant a warrant. That is lacking at the moment. Politicians vary enormously in their skills and may not be the best people to have that sort of last word or ruling.

David Davis: Our approach to this and that of some of the Commonwealth countries is based on the royal prerogative concept of government. That it adds accountability I would dispute absolutely. Jack Straw always used to say that when you are in trouble, the safest place to be is the Dispatch Box of the House of Commons. That is certainly true when it is a terrorist event. I was the opposition spokesman who responded to Charles Clarke on the day of the 7/7 attack, and you can be quite sure that the aim of the Opposition at that point was not to embarrass the Government; it was to show solidarity against an outsider. That always happens. You may remember Gibraltar, when the Labour Party was very supportive. Even though there were some doubts on the day, they were very supportive. Even a few weeks ago when we had the drone attack, there were some differences between the Prime Minister's approach in the Chamber and what was written to the United Nations, but nobody went for that, because we and the public take a view on this.

Secondly, when it comes to warrants, it is very often illegal for the Minister to talk about it publicly anyway. I suspect that you have had some Ministers in on this. It is legally forbidden to talk about it. The pressure on a Minister to be accountable is near zero. If you look in *Hansard*, you will find a number of Parliamentary Questions from me asking the mundane question: what law, what statute, was this done under? I got the answer that we never comment on security matters, so we do not even know. That is how accountable it is; we do not even get an answer about which statute is being used.

First, the accountability argument is a chimera. It is a problem for countries such as the States, which takes a very different view of the royal prerogative than we do, obviously

given their foundation. Many of them view the idea of ministerial approval as being rather flawed.

To take up the Baroness's point about skill, we are very unusual at the moment. We have a competent Home Secretary who has been there for over five years. When I was shadow Home Secretary for five years, I had four opponents, one after another—Blunkett, Clarke, Reid and Smith. The typical tenure of a Home Secretary is about two and a half years: a year getting into the job, a year understanding it, and then they are on their way. What do they do? What does this warrantry process consist of? There were 2,345 warrants last year: 2,700-odd in total, but 2,345 signed by the Home Secretary. That is about nine a day on a working day, if you assume that she signs one or two before going to church in a hurry on Sunday. It is about nine a day on working days, 50 weeks a year. That is not long enough to do this. Fifteen or 20 years ago, there were about 1,000 a year. I spoke to one of the Home Secretaries who did it then. He said that even 1,000 a year was too many. You never got enough information to make a judgment; you got a précis of the case. You cannot make a judgment on something as intrusive as this on a précis. You get no chance to do much cross-questioning.

Victoria Atkins: Which Home Secretary is this?

David Davis: You will have to call him yourself.

Victoria Atkins: I cannot if you have not told me.

David Davis: I am not going to tell you without his permission.

Victoria Atkins: This is hearsay.

David Davis: No, I am just telling you. You can work it out if you try a little. One thousand a year is what they did then. It is now at 2,500 and going up. From that point of view, compare that against using a judge or a panel of judges. First, they are more expert. They are in the job for a long time. Look at the example of SIAC. If we were smart about it, we could do what the Americans do and effectively put up a special advocate to challenge and make sure that the public interest is maintained. That is the way to do it. That is much more effective than this way. I am afraid that this way will improve it slightly, but it misses the optimum outcome.

Victoria Atkins: A simple question: who judges the judges?

David Davis: We are going to have a whole new procedure in place of other judges. Most judicial systems have a structure to them where things are reviewed further up. That is what has happened here. That putting-together of the overarching commissioners, by the way, is a very good bit of the Bill. That is straight out of Anderson, and Anderson was exactly right.

Baroness Jones of Moulsecoomb: What we are talking about here is high-level authorisation. I heard the police officers talking earlier about who was going to be able to give such authorisations, and it can in fact be at a much lower level. A detective sergeant was found last year giving out authorisations.

Victoria Atkins: Was that of intercept warrants?

Baroness Jones of Moulsecoomb: Yes.

Victoria Atkins: That is not my understanding.

Baroness Jones of Moulsecoomb: No, but it is an indication of where a structure can break down, because that detective sergeant did not even know that journalists had a duty and a right to protect their sources. Things can decay in use, which is my experience of the Met Police.

Victoria Atkins: Is the proposed procedure for urgent applications for warrants for intercept, part 1 of RIPA, appropriate?

David Davis: We have different views on this, as is apparent from the answer to Lord Butler earlier. I think it is broadly appropriate. Five days is quite a long time, even in the Civil Service, so it could be shorter than that, but as I said we should publish the number of times we use these every year. We should establish some clear criteria. Obviously in an imminent life and death situation it is a no-brainer, but there are a few others that may not be quite so clear-cut. The London/Glasgow bombing is one example. It was not imminent life or death; it was 12 hours or whatever it was before the attack, but those hours were slipping away. They needed to move quickly with what information they had, and it is very hard to legislate for that, so you have to allow a little tolerance in the urgency. There may also be some circumstances in which there is the possibility of losing information. Information is only available for a very short period. Just those three completely different criteria demonstrate that urgency is rather hard to define. It is very easy to recognise and hard to define, but we could certainly write a statute to cover that.

The Chairman: What you are saying, Mr Davis, is that with regard to the urgency, in your previous answer to Lord Butler, you would advocate first of all that the time of five days is shortened and, secondly, that there might be some special investigatory process for those urgent ones to ensure that they have been dealt with properly, as urgent.

David Davis: That is right. The other thing that I did not mention, of course, is that under my preferred approach, which is a permanent on-duty judge, you are going to have less of a problem most of the time, unless we are happy to wake up the Home Secretary every moment of the day and night. You would have a 24-hour panel. You would still need a process, but it is the sort of thing that I would only expect to be used relatively few times a year—single to double figures, no more than that.

Suella Fernandes: Just to follow up on this, have either of you ever authorised any warrants?

David Davis: I have refused to authorise one.

Suella Fernandes: Is that to be read that you have not been involved directly with any authorisation of warrants in your roles?

David Davis: Yes, except for the one occasion.

Q179 Stuart C McDonald: You have both made pretty clear your views on having this double lock of first a politician and then a judge, but assuming that we retain that double lock, what standard of review is appropriate?

David Davis: This has been quite an area of argument, of course, because the Bill states judicial review standards. Of course, that leads you down all sorts of routes. If you take Wednesbury standards, which is a sort of procedural, "the Minister must have been out of his head", clearly that is not good enough, as often as that may happen. The real standard, and why I wonder why they put in judicial review standards, is that basically it should be a judgment about necessity and proportionality. That is what should be there. There have been debates. Have you had David Pannick in front of you?

The Chairman: No, we have not.

David Davis: You have had people quoting him, I am sure. He says that in these cases it is not really Wednesbury; it really is proportionate when it involves human rights. He was citing cases where people's liberty was at risk, basically in SIAC and so on, which is quite serious. In the very next paragraph of his article, he talks about how judges do not like to overrule the Executive, the Ministers, particularly when it is a matter of national security. You have a balance both ways. One of the things that this Bill needs is absolutely explicit explanation of how the judge will make the decision so that there is no doubt about it. I also think there is a problem about the judge going immediately after the Home Secretary. It is a pretty brave judge who turns over a Home Secretary.

Baroness Jones of Moulsecoomb: I feel more or less the same way.

Stuart C McDonald: The two former Secretaries of State who we had before us were both horrified at the notion that you would have detailed or intensive scrutiny of decisions involving things like life and death, but you seem to be the opposite way round: these are the ones that would require a higher standard of scrutiny from judges.

David Davis: Can you say that again? What did they say to you?

Stuart C McDonald: They seemed to be aghast at any sort of notion that a judge would engage in a very strict and detailed scrutiny of decisions on imminent matters of life and death, for example.

Baroness Jones of Moulsecoomb: Judges are trained to assess evidence and to assess whether or not a course of action is appropriate. I would argue that that surely is a better route.

Stuart C McDonald: You would essentially want the judge to make a decision fresh themselves, based on the same evidence. It is as simple as that.

David Davis: If you really had to have a double lock, which is a silly title for it—it is more like a loose latchkey—I would put the judge first.

Q180 Suella Fernandes: You have mentioned David Pannick's article, but we have heard evidence from Lord Judge, who is the former Lord Chief Justice and head of the judiciary, and Sir Stanley Burnton, who is the Interception of Communications Commissioner. They

both, as senior judges, have experience in this area of law. They have both said that the judicial review test here necessarily imports the test of necessity and proportionality, and that it is the right test that strikes the right balance. Are you disagreeing with them?

David Davis: Yes, I am. Let me give you an example of why, from the intelligence area but not from intercept. In the case of Binyam Mohamed, when the Court of Appeal was considering whether or not to put into the public domain a five-line summary—nothing harder than that—of the fact that the British state had likely been colluding in torture, it took them months to get round to doing it because they were so reticent about overturning the opinion of a Foreign Secretary. They did it eventually only when an American court published the hard data. Even then, they redacted from their own judgment comments about the agencies. Now, that is a very good parable, but it is not the only one of judges being very cautious, and you can understand why, about critiquing an existing government decision, an existing Secretary of State's decision, particularly quickly and particularly with national security. They are just as susceptible. They are not saints. Judges are as variable as Ministers in some respects, but they are human. They do not want to be the person who says, "No, you cannot do that", and then somebody gets killed. After all, at the end of the day, that is the core question in all this.

Suella Fernandes: Do you not think that, for transparency purposes, if there is a threat of an imminent attack, for accountability, legitimacy and reassurance for the public it is the Home Secretary, a Minister, who will need to face members of the public on making a decision, not a judge behind closed doors.

David Davis: The Americans do not find that.

Suella Fernandes: We are not America.

David Davis: No, I am giving you an example of where it does not happen. The Americans do not find that. Nor have I seen a single example in my time in the House of a Minister being held to account for a failure of the services—just the reverse. Go back and look at 7/7. The Opposition very carefully, some may remember, did not call for an inquiry into that. Why? The actions of the political body, in toto, were to act in solidarity, not to challenge each other at that point. The accountability argument does not stand up. I do not think that the public are even aware, most of the time, of individual warrantry.

Also, we are talking about terrorism. Let us be clear about this, because I may have a different view from other members of this Committee: terrorism is not a war, it is a crime. By calling it a war, we give advantage to the other side. It is a crime. We do not require Ministers to sign off warrants on other crimes. I do not see why the public would necessarily expect them to sign them off on this. What the public wants is a safer outcome with the minimum of intrusion into their lives. They will not be worried about the procedure.

Baroness Jones of Moulsecoomb: There is also the fact that it is very hard for any Home Secretary or any Minister to say no to the security services, if they are saying, "You must do it. You have no choice". I would have thought it would be far better to rely on a judge having looked at the evidence and assessed it properly.

David Davis: I do not necessarily agree with that, to be honest. The current Home Secretary does say no to some.

Baroness Jones of Moulsecoomb: I would agree that Theresa May is doing a splendid job.

David Davis: That was not the point that I was making. She does say no to some. The one I am unwilling to name, but I will ask if he wants to name himself, certainly said no to some, more than some, so I do think that they take it seriously, but I just think that they are making a decision on a précis. This is a life-changing decision, and it is sometimes a life-saving decision, on the basis of a précis.

Baroness Jones of Moulsecoomb: I did not say they would not. I just said it is hard.

Victoria Atkins: Mr Davis, you said that it would be a brave judge who stood up to the Home Secretary. Does that not undermine your argument that judges should be solely responsible for this process, because if they are not brave enough to stand up to the Home Secretary, the Foreign Secretary or the Northern Ireland Secretary, one wonders how much they are adding to the whole process?

David Davis: They are good and poor procedures and this, in my view, is a poor procedure. That is the point. What pressures are built into the procedure? You design judicial procedures to give a fair outcome, and you should design these procedures to give the best outcome, the optimum judgment, from the judge, and this is not the way to do it.

Q181 Lord Strasburger: I have a slight change of tack. Some jurisdictions have a method for informing those who have been subject to surveillance after the event, after the case has concluded, thereby giving them an opportunity to seek redress, perhaps in our case through the IPT or perhaps through normal courts. Do you have a view on that?

David Davis: Yes. In the countries that do that, it is quite constrained. Obviously if somebody is still subject to investigation, it is never going to happen. If there is an ongoing case still, it is never going to happen, and even if it is the next-door neighbour it is not going to happen. Nevertheless, the existence of such a procedure is a very good discipline on the agencies themselves and on the people making the decisions, because that way mistakes will out eventually. Frankly out of all of them, only a relatively small number are ever declared, but the existence of the procedure is quite good.

Q182 Shabana Mahmood: I just wanted to return to this whole politicians against judges argument. Is the whole point not about political accountability—the "who judges the judges" question? The politician in this scenario is trying to achieve something different, which is a unique threat, a unique capacity for scale of death and slaughter, and making a decision very quickly. The judges are fundamentally doing something very different, which their training teaches them to do. It is fundamentally different from the politician's job. Why do you think that political accountability should go from a process that is only about judges simply applying the letter of the law, making a judgment on the day, but not worrying about any other of the ramifications that that might have for our national security?

David Davis: I think I have said twice now, so forgive me, Chairman, if I am repeating myself for the third time, that the operation of the House of Commons in particular, in terms of effecting accountability, and indeed the operation of the British media, because

the British media also go shoulder to shoulder when this sort of attack happens, is not one that delivers conventional accountability. Let us imagine for a second that we had a Spanish situation. One reason why, when I was shadow Home Secretary, the Conservative Party redesigned our approach to what we would do in the event of a terrorist attack was because of what happened in Spain. As it happened at the general election in Spain, I thought it might happen at the general election in Britain, so I thought, "This is not going to happen in Britain".

Let us imagine for a second that it did and that we tore into the Home Secretary of the day because the agency had fallen down on this, that and the other. The truth of the matter is that they did fall down on some things. I am not going to replicate them here, but they are easy to look up. The last thing we would be worried about is who signed off the warrant. It would be what did not work. What did not work? We know what did not work. They had information about Mohammad Sidique Khan. They had a photograph, and they cut it the wrong way and sent it around in an unrecognisable form. This procedure does not add to the accountability. It seriously undermines the effectiveness of the process.

Shabana Mahmood: Your argument is a very compelling takedown of the political class being a bit rubbish, which we may or may not agree with. You have a point about accountability, but is that not a better argument for improving political accountability in the system, making us work harder in the Commons and making us work harder as an opposition, rather than saying politicians are rubbish, so let us just hand it over to the judges, who apply a whole different set of principles?

Baroness Jones of Moulsecoomb: I am not saying that politicians are rubbish. I am saying that they are only as good as the information they are given. Quite honestly, having watched the Met over the past 16 years, I know that they can be extremely selective about the information that they give you. That may not be true for the security services; I do not know, but I think it likely is.

Shabana Mahmood: If we accept rubbish information, we are failing to do our political job. I still have not heard an argument that says that we should move away from the realm of political accountability to legal accountability.

Baroness Jones of Moulsecoomb: We do not know it is rubbish.

David Davis: That is to misrepresent the argument. The second legal issue here is that I think you will find that for most of these warrants they are forbidden to tell anybody, even the House of Commons. Again, go back and look. I have not read that piece of the Bill—the 299 pages. I cannot remember what it said on it anyway, but most of the time these warrants are incapable of being put in the public domain. You have a problem there too.

Accountability does not work at this level, and you have to ask yourself at the end of the day what you are trying to do. You are trying to have a counterterrorism policy that works and is very effective against terrorism, and works as well as you can make it in relation to the protection of privacy. Those are the two things. We are trying to find an optimum in that. Nobody says that either side has an absolute, I hope, but we are trying to find an optimum in that. The optimum seems to me to be much better with a fully trained judge, with lots of time, with a full case, at any time of night or day, because you will have a

panel of them, possibly with a special advocate to argue the counter case. That is guaranteed to make a better decision than a Minister.

Q183 Lord Strasburger: I have to say that the Bishop and I are the only people here on the panel who are not politicians. Some people have suggested that a way out of this conundrum is to keep the Secretary of State involvement in cases of national security and leave it to the judges for the rest. Would that open it up for you?

David Davis: The ISC set one level. I think it was just taking crime out of it. RUSI set it a bit higher, at national security; and Anderson set it a little higher still, effectively at defence and foreign. Anderson had a good argument when it came down to what I think of as the Angela Merkel conundrum. If you are going to bug a foreign Head of State, and I am sure we do not do that, there are political consequences. There are diplomatic consequences to almost any foreign operation. I would have a rather different approach. In fact, the approach in the Bill is okay for foreign operations, so I would draw it somewhere there. I have forgotten who said it now, forgive my poor memory—too much German wine—but somebody said, "foreign and significant people in the UK". I do not accept that one. I think that would be a very bad idea, because you would get back into all the establishment stuff. Broadly speaking, I can see a very strong argument for foreign, but outside that, no.

Lord Strasburger: What about national security?

David Davis: National security is such a hard thing to define. If you are talking about terrorism, whatever the Prime Minister says we are no longer talking about an existential threat. This is not the Soviets or the Nazis. In those circumstances, you could see some sort of argument for clearly defined national security. National security is a very broad-based thing now, with a very small number of targets. I would be inclined to say that you would have to have a narrower definition of that for me to be sure.

Baroness Jones of Moulsecoomb: Perhaps I could note two problems with that concept. The first is that definitions are not defined clearly enough, whether we are talking about national security, operational purpose or whatever. The definitions are, at times, quite slack. The second thing is that intelligence is likely to be shared. There is no limit on sharing information with our allies, for example with the Five Eyes. That is a big problem. It is all very well to accumulate information on what we see as our own national security, but will it impact on others?

The Chairman: We move now to the non-political Bishop of Chester.

Q184 Bishop of Chester: I have been thinking that if we had had Owen Paterson and David Blunkett with the two of you, we would have needed a week for the meeting. Owen Paterson gave an impassioned defence of accountability at the Dispatch Box as being the appropriate accountability in a democracy.

David Davis: Did he give an example?

Bishop of Chester: When we had Lord Judge, any suggestion to him that the judge would not be entirely independent and able to stand up to all comers was regarded as an offensive suggestion, not least from someone like me.

David Davis: Judges are all saints.

Bishop of Chester: This was what Lord Judge said. Given the architecture as we have it, how can we improve and turn the latchkey into a double lock, as it were? The judges are appointed by the Prime Minister, not the Judicial Appointments Commissioner. They are reappointed every three years. Is there a way of taking the architecture, flawed though it may be, and strengthening it, making the judicial thing stronger and more independent?

David Davis: You cannot make it the best in the world. You cannot make it world-leading, which is what is claimed for this. Mind you, Malcolm Rifkind claimed that the last system was world-leading too, so you cannot make it that. If you want to improve at the edges, then certainly have a judicial appointments panel appoint the relevant judges. It is a technical decision, not a political one. Certainly have longer tenures or maybe even single tenures. Judges I know are inhumanly strong, but they may unconsciously be affected by that.

One of the things in the Bill that I thought was a very bad idea was that in effect it looked as though the Home Secretary judge made a decision on the funding, and it should not be done that way. There should be a Barnett formula for security, where the fraction goes: if you increase the size of the intelligence budget or the secret budget, you give 0.1% or whatever it might be. Make it a formula. Alternatively, you should have a direct negotiation between the lead judge and the Treasury. You must not have the person being checked up on deciding on the funding. Lord Butler would recognise an NAO model, basically.

Q185 Matt Warman: Do you think that this Bill adequately enshrines the Wilson doctrine in statute?

David Davis: Lord Wilson died a long time ago and so did this policy, I think. The Wilson doctrine has always been a very tenuous policy. It is always down to, "If I do this, I will tell the House when I think it is appropriate". That is almost certainly not soon in most cases, by which time the individual Prime Minister has moved on. I would be amazed, to be frank with you, somewhat shocked even, if in the classifications no Member of Parliament had ever been intercepted. I can think of some good reasons over the decades, so I do not think it is quite what it is seen to be in the public domain. It is not a ban on intercepting MPs at all.

In fact, I would take this away from the Prime Minister altogether. I can see even less reason for a politician to judge on whether or not you should tap a politician's phone. If you think of the arguments we have had in the last few weeks, Jeremy Corbyn has been called a threat to national security. Now, I guess it was just hyperbole. Nevertheless, it introduces a question as to who should do this, so it seems to me there are different criteria—and by the way, they are different from what is written in the Bill, too. The Bill says "MPs and their constituents". In a way, the MPs-to-constituents link is almost the least worrisome, because it is the least interesting to the agencies. MPs to whistleblowers, MPs to journalists, in fact MPs to anybody is what I would make that, and I would make that criterion high.

It is not just MPs, mind you; this is a general privileges issue. With journalists, of course, the Government jumped in and fixed straightaway. You can guess why. The group you are looking at is lawyers, MPs, doctors, clerics and journalists, and none of them should be completely immune. I say that, but again, Chairman, you may remember that at one point some of the terrorist groups in Northern Ireland used doctor's surgeries' receptionists as handoff points, so you cannot make anybody immune, but you have to have a significantly higher threshold, and it really has to be a judge who decides. That is how I would deal with it.

Baroness Jones of Moulsecoomb: I have asked the Met about this and they call us privileged people, those people who come into this group of having certain rights, duties and so on. They apparently do not have a list of us. Obviously that list would change all the time in any case, but they do not have a list, so it is down to the authorising person checking whether or not this person might be a privileged person and whether or not the Prime Minister should be told about the warrant. It is all very specious, I would say.

David Davis: Chairman, I have forgotten one point. One of the things that has become apparent in the last couple of years—it has always been true but has just become apparent—is that communications data is not subject to the Wilson doctrine. Now, communications data is much more important now than intercept, particularly if you are talking about whistleblowers. We have just changed the law in the last year or two, Chairman, to make MPs prescribed people, from the point of view of whistleblowers, and provide them with employment protection. If a whistleblower comes to an MP, he or she gets protection. This is important.

In the Damian Green case, you may remember that Damian Green's arrest was after a whistleblower in the Home Office was in contact with him. That is precisely the sort of thing you have to protect, so the Wilson doctrine has to apply not simply to intercept but to all categories covered in this Bill.

Matt Warman: As I understand it, you are suggesting that these privileged positions should, in particular, be solely a judge, rather than having two politicians, as is currently proposed in the Bill, rather than one.

David Davis: Yes, I would do that.

Baroness Jones of Moulsecoomb: Yes.

Matt Warman: You have said that you would extend that to journalists. Would you care to have a stab at defining a journalist in the modern age?

David Davis: No, I would not. I will leave that to parliamentary draftsmen. The most important group for me is lawyers. Let me tell the Committee why, because this is another of these areas where the Government have the threat back to front. The simple truth is that when you were in the Cabinet, Chairman, the rule was that if a criminal was being intercepted and started talking to his lawyer, the tape was switched off and the intercept was ceased at that point. That was the rule, as it was understood by the Home Secretary in your day. That is no longer true. The IPT's inquiry into this metamorphosed into the data being recorded but kept in a flagged privileged way, and not shown to the prosecution

counsel in any case. Now that is not true and the data is made available to the prosecution counsel.

Now, at some time or another, when one of these comes out, we are going to have a hardened terrorist released on to the streets because of the failure of equality of arms in British law. This is madness. How that metamorphosis happened, I do not know, but it has happened broadly in the last decade or two and it seems to me that we really have to fix that. This Bill has to fix that.

Baroness Jones of Moulsecoomb: This area is so incredibly complex. Lord Chairman, you asked at the very beginning if this Bill is even suitable. I would argue that circumstances have almost moved beyond the Bill at this stage. I took the liberty of sending some of you an encrypted email yesterday and, quite honestly, any criminal or any terrorist could do exactly the same. This Bill will not deal with that sort of thing.

The Chairman: That was a fascinating and a lively debate.

David Davis: It was better than the Berlin Christmas market.

Baroness Jones of Moulsecoomb: I am not sure if it is better than a Christmas party.

David Davis: Chairman, if there are a few issues you have not covered—and I know we are tight on time—can I write to you?

The Chairman: Of course. That applies to both you and Lady Jones. If there are things you would want to add to what you have told us this afternoon, you would be very welcome to do that.

David Davis: It has been a real pleasure, thank you.

The Chairman: Thank you very much indeed. We are grateful.

Witnesses*:* **Peter Carter QC***,* **Martin Chamberlain QC***,* **Matthew Ryder QC** and **Graham Smith**, Partner at Bird & Bird LLP

Q186 The Chairman: A very good evening to you. I am sorry that we are a little later than we thought, but we have had a couple of fascinating sessions. I have not the slightest doubt that this will be equally fascinating. You are all most welcome to the Committee. As you know, in these situations different Members of the Committee will ask different questions, but I am going to ask a very general one, which perhaps gives you an opportunity to make a general comment on the Bill that the Committee is considering, if you wish to. Aside from the new powers on the retention of internet connection records, in your view, does the draft Bill consolidate existing powers or extend them? In answering me, if you wish to make any more general comments, please do so.

Matthew Ryder: The answer to that question depends slightly on, when you talk about extending the powers, whether you mean extending what the security services and the authorities are already doing and what they say is authorised, or what others would say is currently authorised under the existing legislation. There is a dispute and lots of litigation about what is or is not currently authorised under the existing legislation.

My view would be that there are a large number of new powers that are not properly authorised within existing legislation. Just to go through them with headlines, in Part 1 of the Bill, thematic warrants are allowed in relation to Clause 13. There is not a thematic warrant provision for targeted surveillance and targeted interception within RIPA. I know that the Government say that, if you cross-reference Section 8(1) with Section 81, you can find group surveillance as part of targeting but, realistically, thematic warrants are something new, and the idea that you could target people as groups by their activity is something new in part 1 of the Bill. It is important because, conceptually, it is anathema to the existing culture of surveillance that has been going since the 18th century in this country. If we are to move in that direction, it needs an informed parliamentary debate about it, to decide if we want to go in that direction.

Secondly, mass surveillance or bulk interception—whatever you want to call it—under Part 2 of the Bill is essentially something new. I understand—I was involved in the case and litigated the case in the IPT last year—that the Government say that bulk interception or bulk collection is permitted under Section 8(4), but there is a dispute about that. There is a case on its way to Strasbourg. It has been communicated in Strasbourg. There are many of us who would say that it was not set out very clearly, if it was permitted at all, in RIPA.

Part 5, on equipment interference, is really new. It has really emerged only since the draft code of practice was published in February 2015 in response to ongoing litigation. It turns out that the Government's position on the existing power is that it is a very broad power, under Section 5 of the Intelligence Services Act, combined with the draft code that they published on the door of the court in February 2015, so equipment interference is new. It is a very significant power that requires a lot of scrutiny and debate.

Part 7, on bulk data sets, is essentially new, has not been regulated before and is not in the existing legislation in any meaningful way. The power to have access to bulk data sets and how they would be defined is something new.

I missed Chapter 2 of Part 6 on bulk communications data acquisition. That is essentially new. In other words, the large collection of communications data in bulk is something that was not clear from any legislation before. That is essentially being regulated for the first time, under this Bill.

Finally, it is arguable—this is more debateable—that Clause 189, which is the clause that has tech companies particularly concerned, is if not new then certainly of new significance, because it requires telecommunications service providers to maintain their capabilities and combines that maintenance requirement that existed in RIPA with a new definition of a telecommunications service and those who are providing that service. It is broadened out by Clause 193(12) to those who are allowing those communications. That means that those companies that simply have communications apps that facilitate communications through the internet, such as Facebook, Apple or those sorts of companies, may be caught in a way of maintaining their capability that they had not imagined before. That opens up the question of whether encryption is engaged in relation to that issue and, if it is not in the Bill as it stands, in due course whether that is a concern. In summary, there is quite a lot here that is very new and these powers are important. They are significant and, therefore, because they are new, they would require debate.

Martin Chamberlain: That was a very comprehensive answer that enables me to be much briefer. The answer to whether and to what extent the Bill contains new powers is very difficult, for this reason. In the run-up to the tabling of the Bill a number of things that nobody knew the agencies were doing, they were revealed to be doing under the existing powers. There has not been time for some of the things that we have very recently found out the agencies are doing to be tested in legal proceedings. I am thinking there particularly about the use of the extended definition in Section 80 of RIPA effectively to enable thematic warrants to be issued, and the use of Section 94 of the Telecommunications Act 1984, which is something we found out about for the first time in the immediate run-up to the tabling of this Bill. As to whether those activities that we now know have been undertaken by the agencies are lawful under RIPA, the answer is that it has not been tested and so it is very difficult to know.

Generally speaking, whether the Bill confers new powers is, with respect, not a terribly helpful question. One of the important purposes of this Bill is to get a democratic mandate for things that have not yet had a democratic mandate. Whatever you might say is the correct judicial interpretation of some of the old powers, certainly it can be said, without any doubt, that quite a lot of the things in this Bill are things that nobody in these Houses of Parliament has examined the justification for, to date. Are they new powers? One can debate that. The courts have not had the opportunity to debate it, in many instances. They certainly are new in the sense that they have not had a democratic mandate, in many cases.

Peter Carter: Needless to say, I agree with all that has been said, so I shall be even shorter, I think. This Bill is important, because it enables the democratic process to take control of what has hitherto, to a large extent, been a hidden exercise of what is known as a prerogative. It is about time that the prerogative powers were brought to heel and this is a good way of doing it.

Insofar as this Bill brings within the ambit of the law practices that hitherto have either been questionable or possibly outside the law, there is a huge amount to commend it. Only if the kind of activities that this Bill encompasses are subject to law and lawful control,

and therefore lawful monitoring, can it be said that these powers are being exercised in a truly democratic way. We need the powers in this Bill, to some extent or another, to combat serious crime, terrorism and actions against the state. The exact extent is a matter for political debate, as well as legal debate.

One of the problems and one of the ways in which the current drafting of the Bill, potentially and exponentially, will extend the powers is in the definitions clause, Clause 195, which includes a definition of data. As Matthew has said, one of the things that appears to be an extended power is the bulk acquisition of data. Data is defined in Clause 195 as including any information that is not data. Therein lies a problem.

Graham Smith: I am going to be slightly longer. I have identified quite a few new aspects that are potentially new powers in this. First, although the question caveats out internet connection records, we do need to understand that, when one looks at Clause 71, which is the power to issue data retention notices, and one compares it with the existing data retention powers in DRIPA, as amended by the Counter-Terrorism and Security Act of 2015, and if one adds internet connection records to that, Clause 71 still goes far beyond adding internet connection records to the existing data retention powers.

Although this has been presented as something to enable the retention of internet connection records, it goes far beyond that in five or six different ways. Perhaps most significantly, the existing DRIPA powers are restricted to a few types of human-to-human communication—internet email, internet access and internet telephony. This would catch all the background activities on my smartphone that happen when it is sitting by my bedside when I am asleep, when I am away from it, whether it is receiving notifications, getting software updates or anything of that sort. It would capture and cover any machine-to-machine communication, which if you look forward to the internet of things would cover my connected home thermostat or my car checking if it needs a software update. Essentially, anything connected to the internet or indeed any other type of network would fall within Clause 71. It now applies to private services and systems, as well as public, and of course the power to require data to be generated for retention, not just retained, is completely new. The previous limitation to retaining data generated or processed within the UK has been removed, so Clause 71 is very much broader than one might think by just referring to internet connection records.

Other new and extended powers are technical capability notices, under Clause 189. At the moment, under RIPA Section 12, capability notices can be given to support interception warrants and nothing else. Section 189 will apply also to all the new types of thematic, targeted and bulk warrants, under Parts 5 and 6, and will also apply to support the acquisition of communications data under Part 3. All of that is new.

In bulk interception, there is a new power. I call it a new power, but it comes as a result of the warrantry definitions; however, there is effectively a new power to extract related communications data from content and to treat it as related communications data. For instance, if I send you an email saying, "Here is somebody's email address", that is part of the content of my email, but the email address can be extracted from the content and then treated as related communications data. That is very significant, because most of the restrictions on examination of content do not apply to related communications data, so it is very significant. That is replicated as well in the new bulk acquisition and equipment interference powers, which talk about equipment data, which is more or less equivalent to

related communications data. There is the power to extract equipment data from the content that is acquired in that way.

Lastly, there is the extension generally through the knock-on effects of the expansion of the definition of telecommunications operators in the draft Bill.

The Chairman: Thank you so much. They were some very useful answers.

Q187 Matt Warman: Given that we cannot agree on what is meant by new, I slightly hesitate to ask this. The Committee has been blessed with lots of different interpretations of what judicial review will mean in the context of this Bill. What do you think judicial review terms would mean, as far as the authorisation of warrants would go, in this new Bill?

Martin Chamberlain: You have just heard from David Davis about Lord Pannick's article in the *Times*, where he suggested that, in this kind of context, the judges would be applying a high intensity of review. One can explain it in this way: whenever a judge is applying a judicial review standard, there is a spectrum of different types of intensity of review. At one end of the spectrum, there is very light-touch review, which David Davis accurately described as, "Don't touch it unless it's totally barmy". Then at the other end of the spectrum, there is a real rolling up of the sleeves, getting into the detailed kind of review, where the judge comes close to substituting his or her own judgment for that of the ministerial decision-maker.

Practically any judicial review practitioner will tell you that, in practically any judicial review case, a key point of contention between the parties is where on the spectrum that case lies. Is it a light-touch case, is it an intensive-review case or is it somewhere in between? David Pannick's article in the *Times* suggests that this would be an intensive review kind of case. David Pannick is generally right about most things, but I would venture to suggest that you need to apply a bit of caution to whether that is correct in this context. Certainly it is true that a warrant authorising interception involves an invasion of someone's privacy, but it does not involve the kind of restriction of liberty that you see in, for example, a control order case or a TPIM.

The Committee suspended for a Division in the House.

Matt Warman: You were in full flow on what judicial review is likely to look like in this context.

Martin Chamberlain: I have explained that there is a spectrum in judicial review, in terms of intensity of review, with very light-touch review at one end and high-intensity review at the other. David Pannick thinks that, because of the privacy context, we would be in the high-intensity part of the spectrum. I question really whether that is correct. The reason I question it is this: the matters under review, under Clause 19, are whether the warrant is necessary and whether the conduct authorised is proportionate. If you just concentrate on that second question, you are asking yourself the question as a judge reviewing this warrant whether the national security benefit to be derived from the warrant is proportionate to the intrusion into privacy that it involves. That is, to my mind, typically the kind of question on which judges will give a great deal of what used to be called

deference—some of the later judgments deprecate that term, but leeway or latitude, however you want to put it—to the elected Minister. That is what would normally happen in judicial review. There is a House of Lords case called *Rahman* that makes that point. Where you are looking at proportionality assessments by a Minister who is accountable to Parliament, you apply a very light-touch review.

The touchstone, if you really wanted to get an interesting answer to this question of where on the spectrum it lies, is to ask someone from the Government what they think and see if they would be willing to give the kind of parliamentary statement that could be relied on in subsequent legal proceedings, to say that what they meant by judicial review was intensive review. I doubt whether you would get them to say that, because I suspect they would want to reserve the position to argue in front of the commissioners that it was a light-touch review that was intended.

Peter Carter: I hope Lord Pannick is correct, but I also fear that it is so uncertain that he may not be. This is not an area in which uncertainty can possibly be allowed to be sustained. One of the problems about judicial review is a problem that was created by Lord Judge last year because, in a decision called *Regina v L*, a decision in the Court of the Appeal in which he gave the judgment, L was somebody who as a young woman who had been trafficked for exploitation. The question was whether it was right that she should be prosecuted for an offence that she committed as a result of her exploitation, which we would now call modern slavery. The issue was what test is to be applied to the decision of the Crown Prosecution Service to proceed with her prosecution, even though all the circumstances demonstrated that she was a victim of exploitation. The test to be applied is one of judicial review.

There was the kind of discussion that we have heard about: on the one side this; on the one side that. Lord Judge said that we are going to apply in this case a test that is not the conventional judicial review; it is something different from that. The difficulty was that he did not say what it was. I do not know anybody at the Bar, who practises in that area of law, who understands what the test with which we are left in that area of law is. What I suggest is that the simplest way of removing this ambiguity is to suggest an amendment that you simply delete the words about judicial review.

May I go back to the stage about how the judicial commissioners will consider this? It starts off with reviewing what? A decision by the Secretary of State. Normal judicial review is a review of a decision and the reasons for that decision. Are those reasons irrational or are they rational? Do they include considerations that are immaterial or are they centred on considerations that are central to the issue in point? I do not think there is any provision in this Bill for the Secretary of State to give reasons for his or her decision. The judicial commissioner will not be reviewing reasoned decision. The judicial commissioner will be reviewing the decision and, therefore, ought to be reconsidering from scratch whether or not it is appropriate to authorise this warrant and doing so by applying the test of necessity and proportionality.

There is one slight twist about this because, by Clause 169(5) of the Bill, "In exercising functions under this Act, a Judicial Commissioner must not act in a way which is contrary to the public interest or prejudicial to … (a) national security, (b) the prevention or detection of serious crime, or (c) the economic well-being of the United Kingdom". I cannot imagine for a moment that any judge or judicial commissioner would act in a way

that is contrary to the public interest, but who is to determine and who is to assist the judicial commissioner on what is national security, what is in the economic wellbeing of the United Kingdom, particularly if the judicial commissioner is not assisted by reasoning from the Secretary of State? If there is to be reasoning from the Secretary of State, how long is this process to take and why not simply remove the Secretary of State from the process?

Matthew Ryder: May I just make two very short points on this? The first one is that the role of the judge in judicial review, when it has been explained, might be slightly confusing in the sense that there is talk about deference. The question might be what the judge would add in making a decision, if he is going to be so deferential. That is to do with the role the judge has in judicial review, versus the role that the judge would have if the judge was having to authorise it themselves.

I have drawn an analogy here, because it goes back to some of the discussion we overheard from the previous session. There are times when this conversation seems as though it is discussing the difference between political accountability and judicial accountability. One has to remember that the authorisation, in this process, is one very small part of an overall operation, the vast bulk of which is not decided by the Home Secretary or a politician, but is decided by police and judges.

For example, Schedule 5 to the Terrorism Act which is the part that controls terrorist investigations, contains a large number of provisions, production orders and search warrants, including producing material from journalists, all of which are decided by a judge. Those can be much more intrusive, in some circumstances, and much more serious than intercepts, but we trust that to the judge. In serious crime operations, we trust search warrants and production orders to a judge, for a judge to make that decision. The judge does that not by deference to a ministerial decision but by having their own role in terms of making that decision for themselves, and it is a system that works very well with serious crime and under Schedule 5 of the Terrorism Act. That is why one can be led down a cul-de-sac in thinking that we are choosing here between a brand new type of judicial authorisation or judicial role, when previously it had always been the Home Secretary. In reality in terrorist investigations and in serious crime, it is judges and police who are having to make those decisions and who are accountable for those decisions—sometimes life and death decisions.

Q188 Victoria Atkins: I should declare that Peter Carter and I were in chambers together. Mr Carter, you have talked about there not being any provision in the Bill that you can identify for the Secretary of State to give reasons. I have to say, listening to that, I thought, "Crikey, this is a lawyer's paradise". Is it not? We heard from Mr Davis earlier. He estimated that there are 2,300 intercept warrants a year that the Home Secretary does, which equates to nine a day, in addition to all their other duties. If the Home Secretary is having to sit down and write out reasons, in the way that you and I understand as lawyers, I fear that would be a real burden, adding bureaucracy in what is a highly dynamic environment. Is it not better to look at the evidence from the security services or whoever is making the application? Look at that and then the judge looks at it again—the same evidence—and makes their decision according to the evidence placed in front of them by the security services.

Peter Carter: I entirely agree. We do not want this to be a lawyers' paradise. It is going to defeat, not assist, the end. If the law is clear, there is less room for lawyers to get involved.

You do not want lawyers getting involved to try to disentangle what ought to be a clear and transparent process for those who need to know about it. My only slight difference of opinion with what you suggested is I do wonder whether the Secretary of State needs to be involved at all, other than in those things that involve the security services.

Q189 Suella Fernandes: I have a question; I think Peter and Martin dealt with judicial review. We have heard evidence from Lord Judge and Sir Stanley Burnton, who have stated that they think it does strike the right balance, but proportionality involves a balancing exercise—a consideration of the objective and whether the objective is sufficiently important to justify the intrusion, whether the measures are directly related to the objective and ensuring that it goes no further than what is necessary. Do you not think that that encompasses a very clear and balanced assessment of the decision to issue a warrant?

Peter Carter: I do and those words are perfect, provided they are left alone.

Martin Chamberlain: I have to say that I am not quite so sanguine that the word "proportionality" necessarily connotes a high-intensity review. Within the case law on proportionality, under the Human Rights Act for example, there is still a very broad spectrum of intensity of review and, sometimes, even though the court is looking at proportionality, it gives the decision-maker considerable latitude. In other contexts, it gives the decision-maker rather less latitude.

The problem with simply saying that the standard to be applied is judicial review is that we do not know what arguments the Government will make to the judicial commissioners, and it is quite possible that the Government will say that this is the context, balancing the needs of national security against the intrusion into privacy, where you have to accord considerable latitude and discretion to the elected Minister, and where the judge really should not interfere, unless the Minister has obviously struck the wrong balance.

Suella Fernandes: Just by way of follow-up, would you confirm for the record that, in the process of judicial review, a judge would have access to the same information that was before the Minister throughout the original decision-making process? Is that your understanding of judicial review?

Peter Carter: Victoria Atkins made the point that this is a dynamic process and I entirely agree it is. Given the reality of the situation, particularly if it is a security service application for a warrant, it may well be that, by the time it gets to the reviewing judicial commissioner, which may be 15 minutes or half an hour after the Secretary of State has made a decision, further information is available. The judicial commissioner must take account of all the information that is then available, just in case there has been a shift—either augmented information or something that turns out to need correcting.

Q190 Lord Butler of Brockwell: When Mr Carter read out Section 169(5), saying, "In exercising functions under this Act, a Judicial Commissioner must not act in a way which is contrary to the public interest or prejudicial to—(a) national security, (b) the prevention or detection of serious crime, or (c) the economic well-being of the United Kingdom", I thought to myself, "Crumbs, that really is going to shackle the judge". It is certainly putting pressure on him to approve the warrant, but then I looked down and Section 7 says that that subsection does not apply "in relation to the functions of a Judicial Commissioner of—(a) deciding

whether to approve the issue, modification or renewal of a warrant or authorisation". Perhaps you did not intend to mean that it was going to shackle the commissioner.

Peter Carter: No, I do not think it is. What I was concerned about was any suggestion, as perhaps had been made by one of the previous witnesses, that judges were going to be bowled over by a suggestion that this is for national security and, therefore, you must not intervene. The point is that the fact it is there will not prevent the judges from having a rigorous and robust appraisal of the information that is before them, before they make an authorisation or not.

Lord Butler of Brockwell: You are saying that this does not shackle the judge. It will enable the judge to reach full discretion.

Peter Carter: I think so. I hope that the reference to "contrary to the public interest", in any circumstances, would not be something that a judge would find difficult to understand.

Matthew Ryder: I was just going to say, in relation to the point you are making and the point made by Ms Fernandes, it is important to bear in mind that a judge in this position may have access to material, but a judge is not making his own assessment of the facts in judicial review. In the situation where a judge is assessing a search warrant or a production order in relation to something very sensitive, like Schedule 1 to PACE, which could be obtaining material from a journalist, or Schedule 5 to the Terrorism Act, which could be very sensitive and very serious, a judge has the evidence but then assesses that evidence. If the judge thinks the evidence is not sufficient, he could call for more or could look at it.

In a judicial review situation, the judge is essentially bound by decisions and assessments of facts that have been made by the Secretary of State and is applying judicial review principles—which, as Martin rightly says, can be on a range of scrutiny—to that assessment that has already been made of the facts.

The final point to bear in mind is that, normally in judicial review, there is an element of an adversarial process. In other words, the judge is assessing it with somebody making representations in relation to the other side. There will be no adversarial process built into this, the way it stands at the moment. You will have a judicial review, but no one putting forward the argument to the judge in a different situation. Now, that is not unheard of; you have that in other situations, but not in relation to a judicial review situation. That is why it is so important, in this sort of situation, for the judge to be able to be hands-on to potentially look at the facts and evidence in front of the judge, for themselves, and make that decision not shackled by any previous assessment that has been made by the Secretary of State.

Suella Fernandes: Do you not think that that will have a negative effect on timeliness and the speed of decisions, in urgent situations when there are real risks, in terms of the quality of decision-making?

Matthew Ryder: It should not do at all. The reason is that it does not have any problem with timeliness in relation to Schedule 1 of PACE. Those can be extremely urgent applications for very sensitive material in the most intense operations. It does not have any problems in relation to Schedule 5 of the Terrorism Act. I could not imagine a more serious situation, where a judge is having to decide on production orders or search orders

in relation to terrorism investigations, under Section 39 of the Terrorism Act 2000, which are then being dealt under Schedule 5 of the Act.

Q191 Lord Strasburger: Not only am I not a politician, I am not a lawyer and I have been struggling through the fog of arguments in this area, since this Committee started to sit. It is only just now that I am beginning to see some light at the end of the tunnel. Are you collectively saying that the solution to this whole problem is to strike out the phrase that includes the words "judicial review"?

Peter Carter: Are you asking four lawyers to agree?

Lord Strasburger: I will settle for your individual opinion.

Peter Carter: My opinion is yes.

Martin Chamberlain: Mine is, too. It would be much clearer if you said to the judicial commissioners what standard you are expecting them to apply. You could do that in various ways. One way would be to get rid of the words "judicial review", which imply this shifting spectrum, without telling you where on the spectrum you are.

Matthew Ryder: I would still be inclined towards judicial authorisation by a judge, rather than judicial approval. I certainly think in relation to police cases that "judicial authorisation" would be appropriate. In national security cases, you can have a different discussion, but my preference would be "judicial authorisation", rather than "judicial approval".

Graham Smith: I am a mere IT and internet lawyer. I would not begin to venture an opinion on this.

Lord Strasburger: May I then ask the opposite question? What do those words add to the Bill? What benefit do they bring, if any?

Martin Chamberlain: The suspicion or the worry is that it may be argued by the Government, once this Bill becomes an Act, that what they add is a clear signal or flag to the judicial commissioner that, when you are examining warrants issued by an elected official, you should back off and not question those warrants, unless the decision to issue them was irrational or something close to irrational. Probably "irrational" is the wrong word, because clearly proportionality comes into it but, at the far end of the spectrum, that is the worry. It would be very interesting to hear what the Government say in response to that. If they were to say, very clearly, "That is not what we intend. We intend it to be intensive review", and if they were to say it in a way that could then be subsequently relied on in legal proceedings, that would be very interesting.

Q192 Dr Murrison: We have moved quite a long way towards the double lock. The double lock was a point of some controversy, but has now been accepted by the Government. It is worth just recording that. What you are saying is that you would be happy with the deletion of Clause 19(2), which we heard, for example from Liberty the other day, would materially improve the Bill and the scrutiny available.

May I press you on this five-day period, during which the judicial commissioner would take a view, albeit in the Bill at the moment a rather limited view, on the authorisation that the

Secretary of State has given? Do you feel that five days is reasonable, since we have heard from others that it is a very long time for a judge to form a view, particularly since he is likely to be presented with the same sort of material that the Home Secretary deals with, sometimes with a very short timeframe? Indeed, that of course is used as a justification for the Home Secretary dealing with this in what have been characterised as emergency situations, not a judge. May I start? This is something that the Bar Council is particularly concerned about. We can see no justification for that five-day gap. The Secretary of State is a single person. Numerous judicial commissioners can be appointed and, no doubt, will be appointed under the Bill. High Court judges are used to dealing with applications of the utmost urgency.

When there is a need for an urgent application, for example a place of safety order or to prevent somebody being deported from the United Kingdom, I am afraid judges used to be wakened at any time of the day or night and can deal with that matter, as a matter of urgency. There is no reason why a judicial commissioner cannot deal with it as a matter of urgency. For example, a judicial commissioner might be in a position, as the Home Secretary probably might not, under the Bill, to say, "Yes, I authorise this warrant and I want you to come back in 24 hours and I will review my decision and how far it had got". There is provision for that in the Bill, but I can see that practice would develop whereby a judge would make an authorisation that was interim and conditional. I cannot see any reason why five days for a warrant that is potentially unlawful can be justified.

The Chairman: Can you suggest a time?

> ***Peter Carter:*** I do not think there is any justification for any time, any delay. The delay, if anything, is going to be with the Home Secretary, not with the judicial commissioner.

The Chairman: The issue is one of urgency here, is it not? These are only urgent warrants. We are not talking about the 2,500 to 3,000 warrants that have to go through the various Secretaries of State. We talk about a much smaller number. Would that make a difference in terms of, I do not know, a day afterwards?

> ***Peter Carter:*** The difficulty about that is that, if it is urgent, you should not prescribe a time limit because, if it is urgent, it must be done immediately.

The Chairman: Indeed, but the issue is if there is a joint authorisation, which there is on a normal warrant, but an urgent one, because of its very nature and what might be happening, the Secretary of State obviously has to authorise. The Bill says you can have up to five days for a judicial commissioner to review that, but you do not think there is any need for any sort of time limit. It depends on the availability of the judicial commissioner, presumably.

> ***Peter Carter:*** There will be a judicial commissioner available at all times. There should be. It may well be that, if it really is urgent, the Home Secretary or the Secretary of State should be, as it were, a bystanding participant and it should be a single, consolidated process.

Matt Warman: How does that work?

Paul Hudson: The principal decision-maker and authoriser would be the judge. It would be subject to the Home Secretary saying, yes, he or she confirms that it is necessary, so you do it the other way round, in a sense.

The Chairman: To put in my own experience, from when I used to authorise warrants as a Secretary of State—very urgent ones, virtually in the middle of the night or something—you are not going to sit there and have to phone up a judge immediately, when something might have to be decided in minutes, surely.

Peter Carter: That is why I am suggesting that the only reason for having the Home Secretary's decision is this double lock process, is it not? The presumption is that the Home Secretary is a politician who is attuned to security needs and would be the first port of call but, in urgent cases, there is no need for that. The first and only port of call is the judge. If the Home Secretary, having been informed of the information says, "Actually, I disagree", which is highly unlikely, the Home Secretary would then have the power to revoke it.

The Chairman: Why are you suggesting that it should go to the judge before the Home Secretary in an urgent case?

Peter Carter: It is because you then have the consistency of every such warrant having judicial approval.

The Chairman: I understand.

Q193 Bishop of Chester: Is it possible to try to situate this whole discussion between the European culture, which has experienced totalitarian Governments and has a suspicion of government with the history of totalitarian interference, and North America, where there has always been that freedom of the individual and a small state. We are somewhere in between. There is a danger of these wide-ranging powers, which you have identified, being accepted too easily, hence the need for some sort of robust double lock and a strong culture of judicial independence in the judicial element, I suggest. One of the questions we have raised is if the judges should be appointed by the Prime Minister or by the Judicial Appointments Commission. Should they be appointed for a single term of office, rather than have to submit to reappointment? There are these sorts of questions. Are there other ways of strengthening that culture of independence that you all want to see in the judicial involvement?

Peter Carter: Given the gravity of the kind of situation that is envisaged in this Bill, I would have thought that the appropriate candidates for judicial commissioners are likely to be High Court judges. It may be that it is because we have all gone native in the profession that we see no reason to doubt the integrity and the robustness of people who satisfy the criteria of appointment to the High Court bench. I do think, though, that there is a potential problem of perception, if not reality, if appointment to the judicial commission is by the Prime Minister, rather than by the Judicial Appointments Commission, with consultation with the Lord Chief Justice. That would be more appropriate, rather than it looking like a political appointment.

Bishop of Chester: Would you review after three years, as is proposed, or is it better and more of a culture of independence to appoint for a single longer term?

Peter Carter: I am not particularly bothered. Others may take a different view about that but, if you are appointing somebody of the category I have suggested, either they will be sitting senior judges, in which case after three years they may go back to their normal judicial appointment; or they may have retired, in which case three years would probably be sufficient for them to feel that they have done their job and would quite like to go and do something else. Potentially, it will be quite an onerous job. For somebody in this position, I do not see that there is a problem about the perception of independence from it being a three-year term, in the same way as, for example, for the appointment of the Director of Public Prosecutions, the term is sometimes three years and sometimes five years. Nobody, so far as I am aware, has made any suggestion of lack of independence as a result of a three-year, as opposed to a five-year, term of appointment.

Matthew Ryder: Three years is a short tenure for a judge and it might be that the Judicial Appointments Commission would be well placed to express a view about that sort of time in relation to judicial independence, because they have done some significant thinking on how long tenures should be for judges, to ensure that judges do not feel vulnerable when they next come up for review.

Bishop of Chester: When they appeared before us, the impression given by the judges was that they generally sided with the application. David Pannick's article referred to that benefit of the doubt or margin of discretion or whatever it was he said. I cannot remember the term you used there. One can see that a certain culture of it being normal to go along with the Executive could develop without quite being noticed. I simply put this up for you to demolish. Others who have sat in those seats would certainly have those anxieties.

Peter Carter: All you have to do perhaps is look at the history of the current Investigatory Powers Tribunal and the independence that has shown in standing up against the Government's attempts to keep secret the unlawfulness of some of the conduct, and the tribunal's insistence on making public as much of its judgments as it possibly can.

Martin Chamberlain: I would agree with that. I do not think you need to worry that the people who are appointed to these rules will slip into a culture of doing what the Executive want. What you need to worry about is that judges, in performing their role, will do what they think Parliament has told them to do. If they think Parliament has told them, by use of words like "judicial review", to accord considerable latitude to a constitutionally accountable Minister, then that is what they will do. That is not because they are unable to stand up to the Executive; it is because they are honestly interpreting what you have said to them. If you do not want them to apply considerable latitude, you need to make clear that they are not to do so. If you make that clear, they will do what you say.

Q194 Victoria Atkins: Lord Chairman, I am very conscious that I am about to venture into a subject in which you are an expert and I am not, but it is a simple question. Have you taken into account the political sensitivities of Northern Ireland and the way the judiciary is viewed by some, in different parts of that part of the country, when assessing the argument that judges should always come first?

Peter Carter: No.

Martin Chamberlain: I have not either, but I would have thought that, if and to the extent that there are elements of the community in Northern Ireland who have less confidence in

the judiciary than perhaps people would have in England and Wales, or Scotland, then one would have thought that those same elements would have a similar lack of confidence or even a greater lack of confidence in members of the Executive.

Dr Murrison: I have a very quick supplementary to that. Do you think then that that is another argument in favour of the Judicial Appointments Commission appointing commissioners, rather than the Prime Minister? If the Prime Minister appoints the judicial commissioners in relation to Northern Ireland, one would also have to involve the First and Deputy First Ministers.

Peter Carter: I first heard that argument raised at a meeting in Portcullis House on the eighth of this month, and it struck me then that I wished I had thought about it before. It seems a very good suggestion.

Q195 Suella Fernandes: The Home Secretary will have the power to amend the functions of the judicial commissioners. How do you envisage that power being exercised and what kind of modification might be envisaged?

Matthew Ryder: I do not know is my answer.

Martin Chamberlain: I would say the same. It is very difficult to envisage how it might be exercised. In principle, it could be exercised to add to the functions or to take away from the functions. One potentially worrying use of the power would be if it could be used to alter the test that a judicial commissioner has to apply when considering or reviewing the issue of a warrant. I do not know whether it is intended to use the power or that the power might be used in that way, and it would be an interesting question to get the Government's view on.

Peter Carter: Can I make a suggestion? It seems to me that the power to modify the commissioner's role should be confined to those roles that are not central to the authorisation of warrants and the continuation or renewal of warrants.

The Committee suspended for a Division in the House.

Peter Carter: I am very grateful for that, because it has allowed me to find my place in the notes. The question was about the Home Secretary's power to modify the role of the judicial commissioner, which appears in Clause 177. In the clause as it stands, there are no constraints as to which role or part of the role the Home Secretary can amend. This means that, if you decide to remove the expression "judicial review", the Home Secretary could, by his or her power of amendment, depending on who it was at the time, put it straight back in again, which may not be entirely satisfactory.

This provision, Clause 177, appears in part 8 of the Bill. There are various provisions there that explain or provide particular functions for commissioners, including that the investigatory powers commissioner in Clause 169 must keep under review the exercise by public authorities of statutory functions, and so on. I can understand why that kind of role or function is suitable for amendment, as circumstances and the law change. What I would suggest is that Clause 177 should be amended by adding the words, in subsection (3),

"This clause does not apply to any function of the judicial commissioner under parts 1 to 7 of this Act".

Q196 Victoria Atkins: I am conscious of the time. Mr Carter, you have written a very helpful paper, on behalf of the Bar Council, regarding legal professional privilege or LPP. Can you help us with any concerns about LPP and investigatory powers and, if there are concerns, how they can be addressed? How would you recommend they be addressed?

Peter Carter: We have concerns, because there is nothing in this Bill that protects legal professional privilege. Legal professional privilege is the privilege of a client to have private communication with a lawyer, to obtain legal advice or for advice and assistance in the course of litigation, whether active or potential. Communications between a lawyer and a client are not all protected by legal professional privilege, and we are not suggesting that all communications between a lawyer and a client should be protected or immune from investigatory powers. For example, the Proceeds of Crime Act makes it quite clear that communications between a lawyer and a client covered by legal professional privilege are immune, but a client asking a lawyer for advice on where the best place is to stash his stolen loot is not. If there was information that led the police or the security services to believe that that conversation was about to take place, then they would be fully entitled, and I would applaud them, for putting in place some of the provisions of this Bill to get evidence that that was taking place.

The difficulty is that, if legal professional privilege, properly so-called, is not recognised as a privilege that needs to be protected, it strikes at the heart of our judicial system, not just the criminal system, but the judicial system. It is the integrity of the judicial system that is one of the guarantors of our state as a democracy.

Imagine the situation if a client in a commercial action were to say to me or one of my colleagues, "I am about to engage on a contract and I need your advice as to the international effects of this. It is with a Russian company. It is very sensitive because I have competitors in other states. Can you assure me that all our communications will be confidential?". Under this Bill, my answer would be, "No, I cannot", because I simply do not know.

The difficulty is that the wording used in Clauses 5 and 65 says that, where a warrant authorises any of the investigatory powers under this Bill, then any action taken in accordance with that warrant is lawful for all purposes. If the warrant authorises the interception or the gathering of data information concerning communications between me and the client, it would be lawful, even though under international law, European law and our historic law, such communications have been immune, as a matter of public interest. The fact that these rights are ancient is neither here nor there; what matters is that they are current and they are important. They are important for the confidence of citizens in the administration of justice.

Interestingly, when David Anderson produced his report, *A Question of Trust*, in a fairly short passage, he described why legal professional privilege is important. He said, if it is apparent that there is no guarantee that legal professional privilege is protected, it will have what he called "a chilling effect" on the relationship between client and lawyers, and their confidence in the entirety of our judicial system.

The Government fight fiercely for its own legal professional privilege, particularly for example when it is engaged in international arbitration. The Belhaj judgment in the Investigatory Powers Tribunal said this, "There was no dispute between the parties", that is between the state and Belhaj, "as to the importance of protecting and preserving the concept of legal and professional privilege". Why, therefore, is that recognised importance not reflected in the Bill? It is in various other statutes, including in the Terrorism Act 2000 and in the Proceeds of Crime Act, as I have already identified, and in the Police and Criminal Evidence Act.

The problem is that there was one clause, in the Regulation of Investigatory Powers Act, Section 27, that used that expression, "lawful for all purposes". The House of Lords by a majority decided that that empowered a warrant to enable the investigating services, police and intelligence services to intercept communications covered by legal professional privilege between a lawyer and a client. In fact, what was uncovered out of that was of precious little significance, but it was a chilling effect. It has had a chilling effect. Those of us who practise sometimes in criminal law realise that what you require is to build up the confidence of a client in order to give robust advice, sometimes advice that they do not want to hear, but they need to hear. If they cannot be confident that the communication is confidential and secret, they will simply say nothing. That does not help anybody or anything.

Why is it not there? It is said by the Home Office that it is all right; it will be in codes of practice. Interestingly, Schedule 6 contains the only reference to something akin to legal professional privilege, and it is in paragraph 4 of Schedule 6. It says, "A code of practice about the obtaining or holding of communications data by virtue of part 3", so it is confined to the powers exercised under part 3, not under any other part, "must include … (b) provision about particular considerations applicable to any data which relates to a member of a profession which routinely holds legally privileged information", which I assume means lawyers.

There are two things that follow from that. The first is that it recognises, as is evident from the proceedings in the Investigatory Powers Tribunal, that the security services have access to sufficient information to be able to filter those communications that are communications with lawyers, so they know which communications are likely to trigger access to data or communications, which are or the subject matter of which is covered by legal professional privilege. They can do that.

Why is it that the codes of practice under paragraph 4 of Schedule 6 are confined to this particular area under Part 3? The codes of practice or the draft new codes under the Regulation of Investigatory Powers Act also have a provision about legal professional privilege, which does not guarantee the immunity of legally privileged material from access by and disclosure to the agents of the state. It simply says it is a serious consideration, before authorisation is given, not only when it turns out that legally privileged material has been accessed inadvertently, as part of a more general and legitimate operation, but even when it has been specifically targeted.

Whether that will survive a challenge in the European Court of Justice or in Strasbourg, I have my doubts. I am not certain about it, but I have my doubts and I have my doubts because, in international and in regional human rights law, one of the critical basic rights is the right to independent advice or advice from an independent lawyer. Advice from an

independent lawyer is going to be worthless if the client and the lawyer believe that everything said is going to be heard by or accessed by the state.

The state, in the cases that are dealt with in the Investigatory Powers Bill, will in most cases, the chances are, face some kind of litigation involving not necessarily the person whose communications are accessed, but somebody else. Eventually, the chances are, the litigation, whether it be criminal or civil, will indeed be between the person whose communications are accessed and the state. The state would not want to be at a disadvantage if another state in international arbitration had access to all its advice. There have been various expressions about the importance of this right over the centuries but, as I say, what matters is its significance now as a right in a democratic society, which is regarded as a guarantee of a democratic principle and a guarantee that citizens are not at a disadvantage in their dealings with the state.

The Chairman: I shall have to curtail things in a second. I am just asking whether your colleagues agree with what you have said on this or have any additional points.

Matthew Ryder: I do not have anything to add.

Martin Chamberlain: Neither do I.

The Chairman: There is no dissention, which is very good. I am going to close the session now. We have, however, a number of questions we would like to put, if that is okay, to all four of you, in writing. I am conscious of your time, but I am also conscious of the fact that I do not particularly want these questions or the answers to them to be missed. If that is okay with you, we will write to you. We are very grateful. It has been a fascinating sessions and a very important session for this Committee. Thank you so much for coming.