HOUSES OF PARLIAMENT

Joint Committee on the Draft Investigatory Powers Bill

Oral evidence: Draft Investigatory Powers Bill, HC 651

Monday 14 December 2015

Watch the meeting

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

Questions 137-161

Witnesses: Bob Satchwell, Society of Editors, **Colin Passmore**, Senior Partner at Simmons and Simmons, on behalf of the Law Society, **Tim Musson**, Law Society of Scotland, and **Andy Smith**, National Union of Journalists

Q137 The Chairman: A very warm welcome to our witnesses today. I know there was not very long notice for everyone, but thanks to all four of you for coming along to give your thoughts on what is regarded as probably one of the most significant Bills of this Session. As in previous sessions and in any similar parliamentary committee, we will ask you a number of questions, which I hope will stimulate your brain cells. We will have a dialogue with you in this particular session about the importance of privilege to the legal and journalistic professions.

I am going to start by asking a question about the legal professional privilege. How do you think the draft Bill addresses the concerns of the legal profession about privilege and the investigatory powers in England, Wales and, of course, Scotland? Does it create any new issues?

Colin Passmore: It falls to me, as the lawyer among the four of us, to see if I can address that. My name is Colin Passmore. I have been a solicitor for 31 years now and I can modestly claim to be an expert on privilege because I write the leading textbook. I am sad enough to know the thousands and thousands of cases on privilege and the hundreds and hundreds of statutes that deal with privilege. What is unique about RIPA and this Bill is that, on the face of it, they do absolutely nothing to address the concerns that the legal profession has about privilege and the way in which surveillance techniques in all their glory can be used to infringe the privilege.

Privilege, as I am sure you know, is possibly the highest right known to the law. It is over 500 years old. It is jealously guarded, not only by the legal profession but by the courts, with the result that there are usually hundreds of cases in London alone every year in

which challenges to privilege are upheld. In addition, in every single statute that confers investigatory powers of any sort, whether we are talking about the police, the SFO, the Revenue, even local weights and measures departments, there is always a provision that actively protects privilege, so nobody—the police, the Revenue—has the ability to force any client to divulge their privilege. The same thing happens in statutory instruments. This draft legislation and its predecessor are unique in that there is nothing in them that protects privilege.

When this issue came before the House of Lords in the McE case from Ireland some years ago, it is fair to say that the legal profession was extremely surprised that Section 27 had the ability to enable the security services, the police and others at least to listen in to privileged communications in certain circumstances. Even the House of Lords in that case indicated a great reluctance to interpret Section 27 as giving the ability to listen in on privilege, but the House of Lords proceeded quite clearly on the basis that this happens very, very rarely. The House of Lords was at pains to say that if it happens on a regular basis there will be a chilling effect on privilege. The chilling effect is really important, because it inhibits the frankness of clients, whose right it is, with which they speak to lawyers. If that chilling effect is in play, it could undermine the right to a fair trial under Article 6, infringing on privacy rights under Article 8, and undermining the administration of justice.

We know now, from cases like the Belhaj case and other cases that have come to light in the last year, that whereas we thought this interference with privilege was very, very rare, it is happening far too often and on a routine basis. In my view and the Law Society's view, unless this legislation is amended so as to deal with privilege on its face, then privilege, this very old and supremely unique right—there is nothing else like it in any form of communication—begins to become seriously undermined.

The Chairman: Mr Musson, do you want to add anything to that?

Tim Musson: Not a great deal, Lord Chairman. My background is not legal professional privilege in the same way as Mr Passmore's. I am here to represent the Law Society of Scotland. It appears that legal professional privilege in Scotland is very similar to that in England and Wales. The differences are absolutely minimal, although it has arisen in a slightly different way. There are the two sides to the privilege: England started on one side, Scotland started on the other side, and they have come together. Certainly the Law Society of Scotland is very concerned about the erosion of legal professional privilege that appears to be quite possible with this Bill. They have great concerns about it, which do not differ in any way from what Mr Passmore was saying.

The Chairman: Picking up on where Mr Passmore finished, and now that you have added to his comments, it is very appropriate for our only Scottish member to come in on the issue of any possible amendments.

Q138 Stuart C McDonald: Mr Passmore, you suggested that this Bill will need some amendments before you are happy with its approach to privilege. Can you give us any more indication of what sort of amendments you think would be required?

Colin Passmore: There is a serious question as to whether there should be a prohibition on interference with privilege at all. Why is this interference necessary? I respectfully suggest that there are not many cases where lawyers, be they solicitors, barristers, advocates, have been found guilty of abusing the privilege. If a solicitor or a client in their relationship with a solicitor abuses the privilege, the privilege falls away. There is something known as the crime-fraud exception or the iniquity exception.

You do not need these seemingly open powers to listen in to solicitor-client conversations unless you have some evidence that there is something wrong going on. There is very little evidence that solicitors or lawyers abuse the privilege, and therefore the power to listen in, to intercept or to hack is simply, in my view, unnecessary. I would be a strong advocate, and the Law Society is a strong advocate, joined by Scotland and indeed other jurisdictions, for having the type of privilege preservation clause that you find in all other statutes, including those that deal with police powers, revenue powers and so forth. I respectfully suggest that there needs to be a provision in here that makes it clear privilege is out of court.

Stuart C McDonald: Are you frustrated, then, that sometimes we hear from the Home Office that they are scared of putting some kind of prohibition on intercepting legal privilege because of the risk of abuse? You are saying to us in effect that that abuse means that the privilege no longer applies.

Colin Passmore: That is my view. I know many lawyers who understand the importance of privilege and its unique status as a means of privacy in communications with clients. Many lawyers whom I know take the obligations that arise from having the benefits of privilege very seriously. I can think of a handful of cases in which privilege has been abused; I am aware of one, which came to my attention this morning, that has just gone up to the European Court of Human Rights. It simply, in my view, does not happen that lawyers abuse the privilege.

Stuart C McDonald: Mr Musson, do you also seek that prohibition in the Bill?

Tim Musson: Ideally, yes, I would seek that. If it cannot be taken as far as that, there become issues about who is competent to permit interception of these communications. It would need to be someone who understands legal professional privilege, and the sort of person involved in this authorisation might not have that knowledge or understanding.

Q139 Lord Butler of Brockwell: Mr Passmore is making the case for prohibition on the grounds that privilege falls away if a lawyer is engaged in criminal activity. In those cases, you would say that there must be evidence that that is happening, but then you are putting too much power in the hands of the authorities, are you not? They say, "We have evidence"—let us say this is the Home Secretary—"and, therefore, please may we have a warrant to listen to this lawyer because we think privilege has fallen away?". Would you not rather have a stronger safeguard than that, a formal procedure that certifies that that is the case, rather than just the judgment of the Executive?

Colin Passmore: That is a good point. I do not make the case just on the basis of the iniquities exception. I make the case primarily on the sheer importance to the administration of justice of the privilege itself. I am very concerned that this Bill has the ability to undermine privilege more generally. With regard to your second point, in the

way this iniquity exception works with, for example, the police, the SFO or the Revenue authorities, when they seek a warrant to go into a solicitor's office, they have to satisfy the judge in the Crown Court that there is a really good case for being able to go into the solicitor's office, knock on the door and start to take papers away.

Forgive me, I am going slightly off your point but I will come back to it. If privileged materials are identified, whether or not the exception applies there is always an independent lawyer in attendance who will do the physical bagging up of the documents or the computer disks, and he or she will later go away to determine whether they are privileged. There should be a check, of course, but a judge is more than capable of looking at the evidence as to whether or not the iniquity exception is likely to apply. Judges are very good at this.

Lord Butler of Brockwell: Would that not be covered by the new procedure under this Act: that if the Home Secretary is to grant a warrant, it has to be endorsed by a judge?

Colin Passmore: Yes, as long as the reference to the judicial review standard is removed— first, because that introduces an element of ambiguity: what is the judicial review standard? I know that eminent lawyers such as David Pannick have written to say that it is fine; I know many others who disagree with that. But I am not even sure why we need that. If the communication that the authorities wish to intercept is subject to the iniquity exception, that of itself should be enough; we do not need a judicial review standard. Does the exception apply prima facie or does it not? If a judge is not happy that the exception applies, the warrant or the ability to intercept simply should not be granted.

Lord Butler of Brockwell: That, if I may say so, raises a slightly different point. I am not trying to put words in your mouth, but I think you are saying that if the judicial review test was removed, you would be content with a procedure whereby the Home Secretary can grant a warrant, provided it is endorsed by a judge, if there is a really good case?

Colin Passmore: Coupled with an express recognition in the draft Bill, in the statute, that privileged material is not available, that would be great. I would be happy with that and I think the Law Society would be.

Bishop of Chester: The closest parallel might be a confessional and a priest. It is humorous on one level but serious on another. It is on a much lower level than legal privilege, but what qualification there is to an iniquity exception is a matter of contemporary discussion. It may apply only to the Church of England, but we have other religious groups in our country now. I would have thought that if we are going to put something in the Bill, in principle we should, I suggest, at least look at whether that is a parallel set of circumstances, because putting a bugging device in a confessional situation raises the same sort of issues in a different context.

Colin Passmore: It does. I am sorry to disappoint you, but the law addresses privilege as a higher right capable of greater protection than the confessional box. It is easier to get disclosure of your conversations with a confessor than it is my conversations with my client. I am not saying it is very easy; it is very difficult, but I am afraid privilege is on a slightly higher plane so far as the English and Scottish courts are concerned.

Victoria Atkins: To clarify, on the point of the iniquity exception, your evidence is that you wish protection to be put into the Bill that reflects the law as it stands currently across all other statutes, so if a solicitor is trying to commit a crime with their client, that information will not be protected by privilege?

Colin Passmore: Absolutely right. It cannot be protected.

Victoria Atkins: You gave the example of search warrants. Interception warrants are a much rarer event even than the pretty rare event of HMRC or whoever going into a lawyer's office. The safeguards are there, surely, for interception warrants, given how rarely, particularly in secure environments and so on, these are used.

Colin Passmore: The occasions that we know of when cases in which the police have sought interception warrants have come before the courts are relatively rare, and you have to go through the Crown Court judge warrant procedure and satisfy the judge that the iniquity exception is likely to apply. I am a long way from being an expert on interception and the security services, but I have been slightly horrified this year at the number of cases, starting with Belhaj and others, that have come before the IPT in which these issues are raised. I am not myself convinced, although I am not an expert—far from it—that these cases are such a rarity. I would therefore far rather the security services et al had in the Bill the clear recognition of just how important privilege is, plus the mechanism of going via the judge.

Q140 Suella Fernandes: Thank you for your evidence today. Do you agree that someone who belongs to one of these professions that we are talking about, maybe the legal profession or the journalistic profession, may also, albeit in rare cases, pose a threat to national security, and in those cases it is important that the agencies have a power to intercept their communications?

Colin Passmore: I find it difficult to think of a case that would be any more than a rarity. I am aware of one case in Northern Ireland, which is the case I alluded to earlier that has just gone up to the European Court of Human Rights, where a solicitor conspired with his alleged terrorist client to bump off a witness. That is incredibly rare. It is so rare it is shocking. I am not aware of any cases where that is likely to happen. I am not suggesting for a moment that every single member of the legal profession in the UK is beyond reproach—of course not—but I find that a difficult concept to get my head around.

Suella Fernandes: Do you appreciate that the agencies have given evidence that they would never specifically seek to acquire privileged material except when they apply for a specific warrant?

Colin Passmore: I would give you the lawyer's answer to that, inevitably, which is that if that is the case, they cannot have a problem with the Bill recognising the importance of privilege. In other words, if they recognise that they do not want privilege, let us put it in here and make sure it is beyond doubt. Then, if there is a circumstance in which the iniquity exception applies, go to your judge for your warrant. If your evidence is good enough, fine, you are up and running.

Suella Fernandes: Lastly, it is always subject to the test of being necessary and proportionate and that the intelligence cannot be obtained in a less intrusive way.

Colin Passmore: That I disagree with. The courts and some very famous names in the judiciary, such as Lord Denning—I am showing my age—and others since have recognised that the consequence of a claim to privilege is that the court, the Revenue and the police are deprived of what they regard as potentially relevant evidence. It is a consequence that we have to face with an assertion of privilege.

Bob Satchwell: I think your question was: could it be possible? It would be foolhardy of me to say that it was impossible, but it would be astonishing. There are so many examples of the way journalists understand and very carefully apply restrictions upon themselves in relation to national security issues through the DSMA committee, through what were wrongly called D-notices, and things like that. We work like that all the time. I have never known of a journalist who would ever have put someone's life or national security at risk inadvertently. What we are concerned about is precisely the point that there need to be very clear procedures and rules if someone is seeking to invade the journalist's activities and his sources. More recently, and perhaps we will come on to this, the evidence has been that some organisations rode roughshod over something that we all thought was accepted.

Q141 Victoria Atkins: What is the legal status of the codes of practice under RIPA?

Colin Passmore: Vague. They are the worst option for dealing with this issue, in our view. We have a problem here at the moment in that the codes of practice that will be developed pursuant to this are so far unwritten, although I imagine they are going to reflect a lot of what is in the present codes. A code of practice is what it says on the tin: it is a code. We have seen from recent cases where the security services have breached the code that there is not really a sanction. There may be some disciplinary sanctions, but we have seen that the remedies available in the ITP are pretty low-key compared with what one might expect to get, for example, in the High Court, where there might be a claim arising out of a breach.

They are clearly not of the status of legislation. In the absence of something in the Bill, something in the Act to be, that makes the status of privilege clear, the code of practice is always going to suffer, in our view, from this weakness that cannot be cured, no matter what you put in it. It is a code. It is slightly better than the *Highway Code*.

Victoria Atkins: Should we not separate between security services and law enforcement on this issue? As you know, under the codes of practice for the Police and Criminal Evidence Act, there are very real ramifications for the prosecution if the police fail to follow the code. The case may be dropped.

Colin Passmore: I totally agree, but the big difference is that the Police and Criminal Evidence Act, or the Criminal Justice Act for the SFO, makes it clear that privilege is untouchable. You have this primary legislative direction that we do not have here, nor with RIPA. Therefore, the codes of practice are bound to suffer from that. The codes of practice currently have all lovely things about privilege, but they are effectively unenforceable. You have to trust the operatives in the security services to make sure that they will obey them and that they will adhere to them. Personally, I do not think that is

good enough when we are dealing with privilege, which as I keep saying is this extraordinary right, which should be protected in the primarily legislation.

Victoria Atkins: What do you expect to be contained in the codes of practice issued under this Bill?

Colin Passmore: That depends what is in the Bill. I would like to see in the Bill: a recognition that privilege is untouchable and that therefore there should be a fair amount of guidance to the security services and others on what privilege is, why it is so important and what the consequences are of coming across it: a very clear statement, if I may suggest, that there is no basis whatsoever for targeting it deliberately; a very clear explanation of what the iniquity exception should be; and a very, very clear statement of the dangers of playing fast and loose with privilege. You may ultimately cause a trial to be stayed because you have interfered with a defendant's right to a fair trial; you have interfered with his or her privilege. There would need to be a lot, in my view, in the code of practice. I do believe that it has to emanate from the primary direction in the Bill as to the importance of privilege.

Victoria Atkins: I have a final question on that. The commissioners will play a very important role under the draft Bill as it stands at the moment. Is it not sufficient to trust them with bearing that very much in mind when they are looking at individual applications, and in due course reviewing how the legislation is being applied generally?

Colin Passmore: The intent of the legislation is that there would be a senior judicial officer, at least at Court of Appeal level or above, so really senior, experienced lawyers. Provided they also have the direction in here that privilege is untouchable unless the iniquity exception is in play, I would be happy with that.

The Chairman: Thank you very much. We turn now to journalistic provision and privilege, touched on Clause 61 of the Bill.

Q142 Suella Fernandes: Clause 61 requires that a judicial commissioner approves the issuing of any warrants for obtention by agencies. What is your view of that safeguard in protecting the media's rights?

Bob Satchwell: Our simple view is that it does not go far enough. Some interim measures have been put in place to do with RIPA and so on, but the difficulty is that RIPA was used—I have always argued that it was misused, actually—in certain cases, some of which became very full of headlines and so on, to get around the good safeguards that are in PACE. A number of examples that learned lawyers have come up with—I am not a lawyer, by the way—show that that happened.

The key point with legislation of this kind is that we know what the basic intention is in these troubled times, but that is why legislation was enacted previously. I remember when RIPA was enacted it was made clear to me by Ministers whom I talked to, and I believe it was the will of Parliament, that RIPA was supposed to be an Act to do with fighting terrorism. We have found that, in fact, it became something completely different.

I start by saying that it is very important that the legislation—with all due respect to those who may have been involved in that legislation originally; no one expected that it would

be misused in the way it came to be misused—is very clear what the ground rules are before you even get to the codes of practice. Codes of practice are fine so long as someone follows those codes of practice. It absolutely needs to understand, as most people understand—it is something I have always had in my mind, and I have been 40 years a journalist—the first rule of journalism: that you protect your sources. That is in other parts of legislation. It is understood in Europe. It is understood in most places. Judges will very rarely make a journalist reveal his sources, and so on. That background has been totally misunderstood by the police for example, who have ridden roughshod over those principles. Somehow it has to be there very, very clearly.

Going back to your previous question about the possibility of a journalist being involved in something that was against the national interest, they have to come up with evidence, not a fishing expedition; it has to go before a judicial authority. What is more, there has to be an opportunity for the media organisation to argue and to explain the case, because it is not just a matter of delving into journalist records or into who those sources are.

An inquiry into certain parts of a journalist's activity may inadvertently reveal a source that the police or the security services are not interested in. That is why it is very important that there is an opportunity to know when the police or the security services are asking for that, and an ability to argue that case.

The Chairman: Mr Smith, do you want to comment?

Andy Smith: Yes, just to pick up and elaborate on a couple of things that Bob has said. The NUJ agrees that, while not ideal, the provision under PACE is one that we have been able to work with. We have been able not only to oppose some applications outright but to use the knowledge that we have as journalists to explain the situation that we are in, so that a judge can make a variation of something in front of him, which, as far as I can see, is very difficult under the framework that you have in front of you. A police force may come and ask for hundreds of hours of video tape and end up with 10 or 15 seconds that the judge considers to be pertinent to the application they have made.

To be clear, what we have under PACE, as Bob said, is: prior notification, which we think is absolutely essential; sufficient information about the application, for instance what other means have been attempted to obtain the information, so that we are treated not as a first resort but as a last resort; the importance of a face-to-face hearing, which is not about journalists having their day in court but about being able to demonstrate, particularly to potential sources of information, that the journalist's commitment to protect their sources goes up to defending them in open court and going to bat on their behalf; and a rigorous right to appeal before approval is granted. Under the draft legislation, there is an ability for the force or body making the application to appeal, but there is no right to appeal for any of the persons affected, simply because they are not told.

The only other point I would make initially is on the business of communications data, as opposed to the information contained in the communication itself. Journalists are in a very particular position, in that very often the information gathered has already been published and the most important thing is the fact of the communication. The communications data is at least as important as the content of the communication, quite possibly even more so, given our commitment to protect journalistic sources. It is a very particular situation that journalists are in in that respect.

Suella Fernandes: I have one final question. Special protection requires special responsibility, and in some professions the communications between the professional and their client are very well-regulated, for example the medical profession or the legal profession. There are regulations covering journalists, but they are very different from the regulations that apply to the other professions. Do you agree with that?

Bob Satchwell: Yes. It is quite reasonable. Journalism is not a profession in the sense that the professions are professions. It is not a closed shop in that sense.

The Committee suspended for a Division in the House.

Bob Satchwell: But I hope that we always act professionally, which is somewhat different. In all the codes of practice that journalists have, whether for newspapers and magazines or in broadcasting and so on, there is a simple recognition that the protection of sources is a moral duty, as it is put. That is recognised by the courts, by European authorities and so on.

Andy Smith: The other thing PACE does is concentrate on journalistic material. If a journalist, however they want to label themselves, is doing anything that is outside of that journalistic function, it is not covered. Bob talked about the times when legal privilege falls away, and, in a similar way, material that the police want to access concerning a journalist doing something other than their job would not be covered.

Suella Fernandes: The point I want to make is that there is much less regulation for journalists compared to the other professions, and the definition of a journalist is not as clear cut as it is for members of the legal or medical professions.

Bob Satchwell: That is true, but just because the regulation is not quite as formal does not mean that it is not followed. In some circumstances, the following of journalistic practice, which is accepted across the industry, is stronger because it is not laid down in legislation. The fact that it is peer judgments means that people will adhere to it.

On the question of sources and the release of information, it has been recognised in legislation and it is recognised in the courts that sources and other journalistic material should be delved into only in special circumstances.

Q143 Matt Warman: I should declare an interest. I am a member of the NUJ, although, I suppose, a recovering journalist. To start off with, what is a journalist these days? Would you include bloggers? Would you include someone live-tweeting this Committee who is effectively a member of the public? Where might we draw that line?

Andy Smith: To go back to what you were saying, there is an interesting debate to be had on that. I have seen various definitions. The advantage of PACE is that it does not define a journalist, and in some ways that is safer. If that definition is to develop as the technology develops, I would rather see that debate happen as a matter of developing case law, which would involve open hearings rather than conversations behind closed doors that make decisions arbitrarily, or not arbitrarily, about whether somebody who, for instance, had a regular blog and followed our own code of practice but was not paid for it would be described as a journalist. Frankly, some very good journalistic work is being done on the

internet by people who are not associated with the traditional media outlets. There is a debate to be had there, but I would say it is developing.

Bob Satchwell: There are probably some common-sense definitions. It is difficult to define now, but, as Andy said, it will be developed in law. That is one of the reasons why there needs to be an ability to argue a case and say whether this person is a journalist or not. That is part of the principle that is there. I can see that some authorities would say, "We did not know he was a journalist. We just did it". That is the difficulty: that people will try to go outside what has been accepted practice in the past. It would be difficult to define absolutely what a journalist is.

Matt Warman: Bearing in mind that as-yet-undefined elasticity, how could we amend the Bill in front of us to achieve some of the things that you are talking about?

Bob Satchwell: There will be a submission from the Media Lawyers Association, which will come back in huge detail on this. Please excuse me for not having all that legal background. They will come up with some very clear suggestions on that.

Matt Warman: Mr Smith, did you want to add anything to that?

Andy Smith: Like Bob, I am not a lawyer. I would not want to start amending it for you, but the principles would involve something like "somebody who is regularly practising" or "employed". Those sorts of phrases would allow you to separate out those who are simply expressing an opinion on a blog on a regular basis from those who are engaged in journalism.

Q144 Mr David Hanson: Could you comment on what happens when a journalist is undercover and is acting as a journalist but is not, to the public knowledge, acting as a journalist at that particular time? The fake sheikh has been mentioned, but there may be other examples that we are aware of. I am interested, again, in the definition in relation to the Bill.

Bob Satchwell: In most cases, they will be employed or commissioned to be doing something undercover, and there will be some governance surrounding that from the person who has hired or commissioned them to do it. There are some difficulties if people are just going off on their own and doing it—difficulties for themselves, indeed—and they do not have the protection of an organisation behind them. That is what normally happens.

Andy Smith: The NUJ code of conduct is very clear in stating that investigations should be done by open means wherever possible and that any subterfuge has to be justified in terms of an overarching public interest, so you cannot simply decide to go away and pretend not to be a journalist because you feel that it will be the easiest way to get hold of the information.

Bob Satchwell: It is covered by virtually all codes across the media that you have to have a very good reason for subterfuge. In the new editors' code at IPSO, it is very clear that there is governance on that: at every stage of involvement in an investigation of that kind, notes have to be taken at the time about what the public interest was. It will be recorded and they will be audited on that.

The Chairman: Thank you, all four of you, very much indeed. It was very informative and very useful, and the Committee will be looking carefully at the written evidence that you will be providing us as well.

Witnesses: **Mark Hughes**, Vodafone, **Adrian Gorham**, O2 Telefonica, **Jonathan Grayling**, EE, and **Simon Miller**, 3

Q145 The Chairman: A very warm welcome to all four of you. As I explained to our colleagues who came in earlier this afternoon, this is a hugely important Bill. We are very grateful to you all for coming along so that we can ask for your views about it and you can put any points to us that you wish. I am going to kick off by asking all of you how extensively the Home Office has engaged with you with respect to this Bill.

Mark Hughes: It is fair to say that Vodafone has had a number of meetings with the Home Office over an extended period. The engagement has definitely been better this time than it was in the previous Communications Data Bill period. It is also fair to say that we still have concerns over a number of aspects of the Bill, so we hope to be able to talk some of those through today.

The Chairman: Generally speaking, you are satisfied with the engagement.

Mark Hughes: Yes.

Simon Miller: Before I answer the question directly, it is probably worth emphasising how importantly we regard all our customers' data security, both in terms of keeping it safe from attack and in terms of how we process it to provide the service and experience our customers want and need, which is done strictly in accordance with law. The levels of engagement have broadly been good. They have certainly been far more extensive than anything we had experienced before from the Home Office and certainly much better than for DRIPA. The engagement has taken a number of forms—and I hope I am not speaking for everyone else here—including large roundtables with the Home Secretary, timetabled sessions and informal bilateral and multilateral meetings.

The one area that has been lacking is tripartite discussions between us as communications service providers and law enforcement agencies, together with the Home Office. It is also true to say that, although the level of engagement has been good, the iterative approach to consultation has revealed a significant number of issues with the legislative proposal that the Home Office has yet to address or has not addressed. These will be fleshed out, I am certain, in the course of this session.

The Chairman: I am sure you are right.

Jonathan Grayling: To echo that, engagement has been positive and significantly better than the Communications Data Bill. There have been some regular timetabled sessions. They have been cross-stakeholder, involving law enforcement, industry and the Home Office. That has been really useful, because it has assisted in providing a common understanding of operational requirements, technical capabilities and policy drafting. That said, this is a piece of government legislation and it is ultimately Parliament's decision what is and what is not included in the Bill. EE's main priority is our customers' privacy, and as such there are still a number of areas in the Bill that we have some concerns about, which we hope we can bring out in the next hour or so.

Adrian Gorham: I will not repeat the comments my colleagues have made, but it is certainly much better than we have seen in previous legislation that has gone through, so we are very pleased about that. We have had a good level of debate.

The Chairman: That is an interesting start.

Q146 Lord Henley: It is very pleasing to hear that the Home Office has been consulting, speaking as one of the various former Home Office Ministers on this Committee. We understand there is a shortage of IP addresses, and we also understand you do not always record which subscriber had which IP address and which port number at any specific time. What can you tell us about the practical difficulties and the costs that might be incurred in conducting IP resolution?

Adrian Gorham: When they developed the IPv4 standard, there were 4.3 million addresses worldwide, so that clearly was not enough, as technology took off, to give each customer an individual IP address. When the mobile phone business moved into doing internet connections, we had to come up with a solution to that, because we could not give every customer their own unique IP address. They developed a technology called network address translation, which means that every time you go on to the internet and have a data session, you are given an IP address, for a very short period, for that transaction, and then it just drops off. The next time you do something, you are allocated another one, so it is very dynamic and it changes all the time.

We had no reason to make a record of that. That is our challenge. We now need to record what number we allocate to each session and store it, and build the devices so that we can disclose that to the authorities.

Jonathan Grayling: To pick up on Mr Gorham's comments, the key point here is that at the moment the technology does not exist to be able to resolve that IP address. The public-facing IP address could have multiple thousands of unique devices attached to it. Indeed, trying to resolve that public-facing IP address to at least a near one-to-one match—and that is Parliament's intention—will require the retention of internet connection records.

As I said, the technology does not exist at the moment. We are in the feasibility stage now. At the end of that feasibility stage, it will probably take up to 18 months to deliver a solution because of the complexity involved.

Simon Miller: There is not much to add to that, other than to say that the technical challenges faced by my colleagues at both O2 and EE are replicated across the board.

Mark Hughes: I have just one thing to add. Vodafone is in exactly the same boat. We do not keep the IP data of all our customers. We are going to have to deploy new technology to be able to do this. The other thing that has not been said so far is that we will need a very big storage system to be able to keep it. It is a significant amount of storage.

Q147 Lord Butler of Brockwell: Could I take a step back and ask about the existing system and the requests you get for call data records under Sections 21 and 22 of RIPA? We know that is a diminishing resource as far as the intelligence agencies and law agencies are

concerned, but are you satisfied that, to the extent you still have those records, that system works reasonably well?

Jonathan Grayling: Yes, the current acquisition arrangements under RIPA work well. One of the primary provisions, which is tried and tested, is the SPOC system. Essentially, that is the provision of comms data to law enforcement and the SIAs to a single point of contact. The use of SPOCs provides a strong, transparent and stringent process. As I said, it has been tried and tested over many years. Their SPOCs are specially trained. They are accredited in the use of CD, so they can advise their respective officers within law enforcement and the SIAs on what CD needs to be acquired.

That said, we also welcome the additional safeguards in the Bill. We welcome the requirement for a designated person, independent from the requesting agency; the streamlining of existing legislation and repeal of old legislation, so the Investigatory Powers Bill will be the primary piece of legislation for the disclosure of CD; and the restriction of ICRs to certain authorities and for certain purposes. Moving into the IP world, keeping the SPOC community and law enforcement up to speed with new technology is going to be a challenge, and a significant amount of effort will be involved in ensuring that law enforcement and SPOCs can interpret the data that we are talking about today.

Lord Butler of Brockwell: Going forward, then, into the new world—you have begun to describe the complexity to us—is it practicable, by using the internet connection records, to distinguish just the first line of the address, which is what the Government want to do, and to draw a line between that and what would be more revealing about the content?

Mark Hughes: This is where we get into some of the more technically challenging areas of the Bill, for sure. It is important that we call this out as it is. We are talking here about web browsing data when we talk about internet connection records, so we need to recognise that this is a hugely sensitive part of the capability that is looking to be developed. In terms of how easy it is, this is where we start needing to talk about over-the-top or third-party service providers, who may be running their communication services under the underlying network providers that are here today.

To try to bring this alive with an example, Vodafone and everyone else here will act very much like a postman today. We would carry a packet of data, or a letter in this scenario, from point A to point B at an IP address. We do not know what is contained in the letter in this scenario. In future, the challenge for us is having to open that letter. Let us say it is a Skype service. We would have to say, "Okay, now we have opened it, we understand that a Skype service is being provided", and the Skype username or ID of the person would be within that. You can already start to see how the lines are being blurred between traffic data and content when you start having to open packets of data as they cross the internet.

One of the main concerns here, especially around third-party data, is that, today, Vodafone has no day-to-day business use for this data. We do not create it, so we are going to have to generate new data about our customers that we do not generate today. Secondly, we do not understand its structure. That structure can change on a day-to-day basis, and it is encrypted, so we will have to be able to strip off the electronic protection and decrypt it before we can store it. We would be concerned about attesting to the accuracy of that information as well. I am also concerned about possibly creating a single point of cyber

vulnerability when you start decrypting things to be able to store them. There is a very good reason why they are encrypted in the first place. I am concerned that we will perhaps solve one problem, but not necessarily in the best way, and create another cybersecurity problem. Our point is that the very best people to keep data about the services being provided are the third parties. They should be the people who are keeping information to help law enforcement fight crime in this country, rather than the underlying service providers.

Lord Butler of Brockwell: Give me an example of what you mean by the third parties.

Mark Hughes: I gave you an example there. It could be a Skype; it could be WhatsApp. It is those types of service providers.

Lord Butler of Brockwell: I see, so the people for whom you are carrying the traffic. Okay. You have talked about this being a very complicated process. Can you give us some idea of the costs?

Mark Hughes: Until we have been served with a notice, I would be purely speculating as to the cost. I would be uncomfortable giving you any kind of idea until the Home Office has served us with a notice. It would be significant, it is fair to say.

Lord Butler of Brockwell: The Home Office produced a figure, if I remember correctly, of about £180 million. Do you think that is an overestimate or an underestimate?

Mark Hughes: Where this figure from the Home Office came from I cannot say, because we were not consulted when it was put together. We were consulted only after that figure was put together. I would not be able to speculate, from a Vodafone perspective, as to how much it would cost.

The Chairman: Would all four of you agree that the cost implications are considerable, significant, huge, something you can manage, or you do not know at this stage?

Adrian Gorham: It is going to be huge. Also, there is the way data is exploding. The increase in data is about 100% per year. That is the big issue with costs; this is going to double by next year, with the way the internet is going. There are going to be big increases in the future, with huge amounts of data.

Jonathan Grayling: I agree. Going back to what Mr Hughes and Vodafone said, unless we can be explicit in the Bill about exactly what data we are going to be required to retain in any future data retention notices, it is simply not possible to give a figure. If there is, within the legislation, scope that third-party data falls into our areas of responsibility, the costs will be even more. We are only focusing on the data that we understand now, the data that traverses our network, the data that we require in order to route a communication and provide a service to our customers. Even then, it is incredibly difficult to come up with a cost.

Q148 Lord Butler of Brockwell: I have one final question. I get the impression that you are not enthusiastic about this provision in the legislation. You think it is a lot of work. Even if the Government meet the costs for you, you are not enthusiastic participants.

Mark Hughes: It is not necessarily about being enthusiastic. We absolutely recognise the challenge that law enforcement and Government have here. Vodafone's concerns are very much about making sure that we have a Bill that is technically workable. At the moment we are really concerned about being able to keep data about a service that is nothing to do with our core business, generating new data about our customers and especially stripping off electronic protection and decrypting communications passing through the internet. This is a highly challenging arena for any of the companies here today in which to do things on behalf of somebody else's communications services. We feel that the third parties providing those services have an obligation here to assist law enforcement fight crime.

Q149 Bishop of Chester: Clause 193 gives a series of definitions in the Bill. One of the issues we have been wrestling with is the distinction between data and content. That is in subsection (6). Are you comfortable with that distinction between data and content in the context you are describing?

Jonathan Grayling: This is an incredibly complex area and, with respect to the Home Office, it is even more complex to try to define within a piece of legislation. Without wishing to go over the ground we have just covered, there are issues in relation to what is perceived as content and what is perceived as CD with respect to who owns that data. The definitions provide a basis for further discussion. It is a starting point, and it is a starting point for defining those capabilities. That said, echoing what we have just spoken about, to a CSP, to a network provider, the communications data is the data that is available to us that we see in order to provide a service to our customers. Essentially, that is the data we need in order to route a communication that we will process and that we will make a decision on. If we do not make a decision on that data, we do not perceive that as being our data. It is simply data attached to a packet, but the data within a packet could be communications data to the sender of that packet.

Again, if you talk about WhatsApp, all we are interested in doing is sending the WhatsApp message that traverses our network to the WhatsApp server. If you were to open that WhatsApp message, you might find out to whom that message was being sent, but we have no need to know that; we are just sending it to the WhatsApp server. That data could, to WhatsApp, be perceived as communications data, but, because we have to open the packet, it is content to us. This is where there are blurred lines and why we are looking for clarity in the Bill as to exactly what data we should be required to retain as communications service providers.

Adrian Gorham: To build on Mr Grayling's point, another issue here will be the encryption, because so much of the data now going over our networks is encrypted by those application providers. In a lot of cases, we cannot see what is contained within that traffic. They are not going to give us the keys so that we can decrypt it to examine it, so in a lot of cases we are completely blind to that traffic.

Simon Miller: The issue here is that there is a clear need for further discussion with the Home Office to arrive at a text that works. There may be a need for further interpretive text, potentially in the Bill, but there is definitely a need for more than there is currently. The introduction of the ideas in the Bill is useful, but they need further unpacking.

Bishop of Chester: Do you think your customers would make that distinction between content and data, or would they think that the data is quite personal to them, quite apart from the content?

Mark Hughes: We know that customers would expect all the companies here today to look after personal information to the highest levels possible. Concerns about decrypting third-party communications as they cross the network would be of a concern. Again, it touches on the point that the persons who should have the obligation here are the third parties. They do not need to break the encryption because they have created the communication in the first place.

Q150 Lord Strasburger: Putting the last two topics together, encryption and degree of difficulty, with the proportion of internet traffic that is encrypted increasing by the day, is it possible that you will end up in 18 months' time with an expensive and rather complex system to collect these internet connection records, a diminishing part of which is of any use because encryption has increased?

Jonathan Grayling: That is a real risk. Technology is moving on so quickly. New protocols, new algorithms on the internet, are being created all the time, which makes it very difficult for us to see those communications. Yes, you have encryption, but you just have the way the internet is developing in itself. I would not like to talk about timescales and I would not like to comment on the actual benefits that the technical provisions we are introducing would give to operational law enforcement and the SIAs, but it is a risk that technology is moving so quickly that we may be behind the curve.

Q151 Baroness Browning: The three-level categorisation of communication in the RIPA legislation has been replaced by two: entity data and events data. Do you feel that reducing these categories down to two levels causes a problem? Are they sufficiently clear and workable? Is that a good thing? Is that going to cause you problems?

Adrian Gorham: In its simplest form, it does not cause us a problem. There are going to be two types of data. There will be entity data, which is about the actual person; it will be your name, your address, your telephone number, so it is about the individual. Then there will be the events data, which describes the event and will be about where something took place, the location. The good thing about those two fields is that a different level of authority is needed by the police if they want that data. If it is about you as an individual, that will be authorised by an inspector, and if it is the broader data that includes the location, that will be signed off by a superintendent. That gives us clarity about what is required. The challenge is that as we move forward and more and more communications are coming online and more and more machine-to-machine, there will be different fields of data and we will have to have regular discussions to find out where those fields sit.

Mark Hughes: We were clear about the previous definitions. We are not clear why it needed to change, but we have no particular objections to the proposed changes.

Baroness Browning: With the advance in technology, are you referring to the fact that things that are not in use now but are coming up over the hill are things you will have to take decisions on?

Adrian Gorham: In the future, you are going to have SIMs in your fridge and your dishwasher. All these appliances are going to have SIMs in them that provide data. That all has to go into this process, and we are going to have to make those decisions where things sit.

Q152 Mr David Hanson: It is important in this session to try to nail down in some detail what you believe the Government are trying to do and whether you can deliver it. Could you just indicate to the Committee your understanding of internet connection records, as of the Bill's description?

Mark Hughes: It goes back to what I was talking about earlier. Internet connection records are web-browsing data, so they are not the page you end up landing on but the domain that you have visited. They do not exist today, so this is about us having to create and generate entirely new data sets.

Mr David Hanson: For Vodafone, how easy is it to deliver that new data set as of today?

Mark Hughes: It is extremely difficult, because, as we have heard, the vast majority of over-the-top service provider data that would be an internet connection record is encrypted and it is not data that we understand or in a structure that we have any understanding of, because we have not created it. We are now going to have to create an entirely new type of data on behalf of another company, decrypt it and then store it ready to disclose potentially in a court of law, where we cannot even attest to the accuracy of that information. It is very difficult.

Mr David Hanson: Vodafone is an international company. What demands are being made on you by other nations outside the UK in this field at the moment?

Mark Hughes: There is no standard approach internationally. There is a real patchwork, depending on the country. There is no one model. The UK model is certainly the most transparent, but there is no one model that fits all.

Mr David Hanson: What is other colleagues' understanding of what an internet connection is?

Adrian Gorham: This still has to be clearly defined.

Mr David Hanson: The Bill is in front of us now. Is it clearly defined for you in the Bill?

Adrian Gorham: We are nearly there on the clarification of what makes up the record. The challenge is that this is something we have never kept previously. We keep your CDR for every phone call you make. We keep the record, we store it for a year, and we can disclose it. This is a completely new kind of record that we are going to be keeping, and then we have to hold it, store it and disclose it, so it is a big step up for us in what we need to do and provide.

Simon Miller: The issue here is that we know that an internet connection record is going to be something like a simplified version of a browser history, but we do not know exactly what it is going to be. Until that bit is nailed down, we cannot ascribe a cost to it or know

exactly how difficult it will be to implement. We do know that it is going to stretch our existing capability many times.

Jonathan Grayling: The key point here is that an internet connection record does not currently exist and we have to create it. Even once created, it may not exist as one whole record. As Mr Gorham said, we are beginning to get some clarity on what the Home Office believes an internet connection record may be made up of, the subsets of that internet connection record. Some of that data may or may not be retained. The issue is putting it all together to try to create something that is going to be of use.

Mr David Hanson: We are the draft Bill Committee. The real Bill Committee will meet in the Commons and the Lords, probably from the end of February until the end of July, and then this will be law. The question to all of you is: are you satisfied that, by the procedure of considering this in both Houses of Parliament, the definition, the deliverability and the apportionment of cost will have received sufficient attention to have confidence among your companies and the public that it is being done to the standard the Government expect?

Mark Hughes: Until the Home Office serves us with a notice as to exactly what it wants, it is difficult to speculate. We all understand it to be web browsing; we know that it is going to be difficult and challenging and that it will create lots of new data, which is going to be highly intrusive, but until we have a notice and know exactly what we have to keep about which companies, it is difficult to speculate.

Simon Miller: There has been a process of engagement in place that has got us this far and has led to improvements in what is being proposed. That suggests that it is possible to get this over the line. However, there are still a substantive number of challenges that need to be met in order to do that. At the moment, we have not necessarily had the responses from the Home Office that we either want or need on this in order to have full faith in that process.

Mr David Hanson: Is that the general view?

Jonathan Grayling: You cannot underestimate the complexity.

Mr David Hanson: Well, let us just go back to the point that Lord Butler made earlier about the costs, again, which the Government have estimated at approximately £170 million to £180 million. We had a panel in front of us last week in another Committee room who basically said that they estimated that they had spent £170 million, just among the two to three companies in front of us that day. Again, it is important that you, either now or before the Bill reaches deliberation stage, as well as negotiating with the Home Office, are clear about the implications in relation to the costs. The Houses of Parliament cannot pass legislation that will not be deliverable, and it is going to have burdensome costs, on the taxpayer, the public, or both. Can you give the Committee any estimate now? Could you tell the Committee, "We think it is in the ballpark figure of X"?

Mark Hughes: Again, without wishing to be evasive on this question, it depends on how much of the internet traffic the Home Office wants us to keep. Is it every single third-party service? How quickly do they want it decrypted? How much of it needs to be stored? Is it for the full 12 months, like everything else? How much resilience does it need? Do we need one set of resilience, or do we need to be able to build it three times just to make sure

that it goes down? Is it that important? It is those sorts of factors that can make this change from one number to something completely different at the other end. The only thing I can say, given what we know is in the Bill and what we know about the technology in this area, is that it will be a significant cost. Saying how much it will be would be me picking an item out of the air and literally speculating. It is going to be significant.

Mr David Hanson: I take it, by the looks of agreement and nods, that that is pretty much where the panellists are. Could I just then throw the other question in, which is still an important question? Ultimately, whatever the cost is fixed at—and you have said there will be a cost—who, in your view, is responsible for the apportionment of that cost? Is it something you take as a commercial issue? Is it something the Government have to fund 100%? Where do you land on that figure?

Jonathan Grayling: We believe that the Bill should make it explicit that a company impacted by this legislation is fully able to recover the costs incurred. We believe that if there is no cap on costs based on a proportionality aspect, and the obligation and the financial impact is simply passed on to the CSP, this could result in delivering disproportionate solutions. If there is a cost recovery model that places a cap on cost and is based upon proportionality, that provides a far safer investment for taxpayers' money and the privacy of our customers.

Q153 Mr David Hanson: Is there any disagreement with that? No. I have one final set of questions. Ultimately, if it is doable, if it is defined, if it is delivered, and if it costs something, at some point a police officer or agency is going to ask you for information. Are you satisfied that the Bill has sufficient provision in relation to the single point of contact from officers? Is that sufficient to give your customers and you the security you believe you would need?

Jonathan Grayling: It goes back to the point that until we know exactly what data we are required to retain and the format that it is going to be stored in, it is impossible for us to say whether a SPOC or a police officer is going to be able to interpret that data, because that data does not exist at the moment. That record simply does not exist, so we cannot say whether a SPOC community is going to be able to interpret, because we do not know what they are going to be able to interpret yet.

Mark Hughes: It is fair to say that the SPOC community will have to undergo an extensive amount of retraining to be able to understand this and make use of it in a day-to-day investigation, especially considering how quickly, sometimes, they have to be able to make a decision based on this data in grave situations.

Mr David Hanson: I will come back to the final point: this could be law, in one form or another, by September 2016. What is your assessment of the deliverability, as of today, of the Bill as it stands?

Adrian Gorham: We would all accept that this is a big step up in capability. Everybody understands the challenge that the police and the security agencies have, and we all understand the capability gap they have with modern communications. This is going to be a step change for us, and that is why the discussions we are having with the Home Office are quite detailed, because we need to get this right. I am sure that everybody else on this panel, as well as me, wants to make this work and to ensure that taxpayers get good value

for money. The only way we can do that is by having the strong discussions now, so we are very clear on what we need to provide and we do that in the most cost-effective way.

Mark Hughes: Regarding deliverability, without wishing to keep harping on about the same point, the easiest and most elegant way to deliver this capability is for over-the-top service providers to have the same obligations as companies here do today to assist law enforcement with information about customers who are using their services who may be breaking the law.

Q154 Lord Strasburger: On the subject of deliverability, Mr Hughes, you have twice said, "Then we will have to decrypt the data". How can you possibly do that unless you get co-operation from over-the-top providers, such as Facebook and others, or you get sufficient information from them as to how to decrypt that data, or from end users regarding how to decrypt their data? How can you do this?

Mark Hughes: You are absolutely right. The point of this is that we will have to be supplied with new technology, from law enforcement or intelligence agencies, to be able to decrypt that information about third parties and store it. That goes back to the point, again, that it is not preferable for our companies—certainly not for Vodafone—to be able to decrypt communications and store this. It would be much more elegant for the third-party service providers to have this obligation to assist law enforcement to fight crime.

Lord Strasburger: Presumably, by treaty, bearing in mind that most of them are American.

Mark Hughes: The Bill itself allows the Home Secretary to place an obligation on any person. Most, if not all, providers—certainly the big ones—have infrastructure and offices here. Given the way the internet is structured, there are things globally; I see no reason why the third parties would not want to assist with helping law enforcement in this space.

Stuart C McDonald: Mr Hughes, I think you said that you would not be able to attest to the accuracy of ICRs. Is that because of this process of decryption, or are there other reasons why you would not be able to do so?

Mark Hughes: It is fair to say that if we were able to extract data belonging to another provider, not understanding its structure as it crosses our network, I would be uncomfortable with being able to explain the accuracy of another company's data. That would be an incredibly difficult thing for Vodafone to do.

Stuart C McDonald: So you might not be able to come up with accurate ICRs at all.

Mark Hughes: An ICR does not exist today. Once it is created and we have solved all the technical challenges that we have already discussed, I would imagine that it would be tested in court once this evidence becomes as bread-and-butter to the criminal justice system as mobile phone evidence is. I would imagine that it will be tested very heavily on the grounds of, "Who created it? How did you decrypt it? How accurate is it? If you did not create it, how can you attest to the accuracy of it?" Companies here, such as Vodafone, have to attend court to be cross-examined on mobile phone evidence that has been collected. We would find it extremely awkward to have to attest to the accuracy of data that we had not created in the first place.

Suella Fernandes: You appreciate, do you not, that the current lack in capability—for example, the requirement to keep internet connection records, or store them—means that the agencies can paint only a fragmented picture of a known suspect?

Mark Hughes: I absolutely recognise that.

Q155 Suella Fernandes: Examples abound, but in a recent referral of 6,000 profiles from the Child Exploitation and Online Protection command to the NCA, around 800 of those could not be progressed because of the lack of this capability. That is about 800 suspected paedophiles who were involved in the distribution of indecent images whose details cannot be gathered by the agencies. Bearing in mind the benefit that is gained by this storage and retention requirement, what alternatives do you think are viable while providing a similar benefit?

Jonathan Grayling: We are not necessarily questioning that there is an operational case for this. We work closely with the NCA; we work closely with CEOP. We are just trying to reflect the technical complexity involved in meeting the demands of law enforcement. We all have a duty of care as operators; we want to be good corporate citizens as well, but if the technical complexities are there, those are the facts, and we are trying to work through those with the Home Office to provide the provision that they are looking for.

The point that you raise there about CEOP goes back to the point about the knowledge of the law enforcement community. Certainly, the NCA are pretty advanced through the CEOP side of things in relation to trying to highlight these gaps in technology, and we work very closely with them on trying to close those gaps, but it is proving very, very difficult. The technology just does not exist at the moment.

Mark Hughes: I absolutely recognise what you are saying. We care passionately about assisting law enforcement. We take extremely seriously all the obligations that are placed upon us, and we do everything we can to give the best service to law enforcement through the system, with the things that we are obligated to do by law. As Mr Grayling has just said, we want to make sure that when this legislation passes and it has gone through the correct level of scrutiny, the obligations are technically workable and we can continue to provide the level of service that the police and law enforcement agencies expect from us. We get how important this stuff is, and we really want to make sure that we can provide the data in the best way. Again, so much of this is going to be about over-the-top service providers that we must make sure it is achieved in the simplest way possible, and the simplest way possible is for those third parties to co-operate with law enforcement.

Suella Fernandes: In terms of maintaining the security of stored data, you use firewalls and personal vetting systems, and those are effective ways of keeping data secure.

Adrian Gorham: All the operators here are very experienced at looking after our customer data. We all have a layered approach; there are different systems and processes for keeping it secure. All this means is that we are going to have even more data that we will have to keep secure.

Interestingly, one of the parts of the Bill talks about a request filter, which will be run by a third party; a third party will take bulk data from us and analyse it for the police, to make

sure the police only see the data they require. My concern there would be that that third party has exactly the same level of security that we deploy ourselves in our businesses. A number of us have international standards; I would expect that third party to have that level of security, if it has my customer data. I would expect the governance that we are putting in place to go and do audits on that third party, and I would—if I am giving them my customer data—expect to be able to go and audit them myself, to ensure that they are living up to our standards as well.

We are all very used to looking after security and protecting that data, but we now, with this Bill, have a third party whom we would need to give data to, and we need to be very sure that the same level of security is deployed there as well.

Q156 Suella Fernandes: Lastly, retention is subject to stringent controls; it needs to be necessary, proportionate, signed off by an independent person, and it needs to be compliant with various case law and the European Convention on Human Rights. What is your assessment of that consideration of lawfulness and effectiveness, combined with the exception of whether it is reasonably practical, as a sufficient safeguard to strike the right balance?

Adrian Gorham: The safeguards in the new legislation are very good. They are much improved on where we are now, and they are much more transparent. We have to ensure that the different auditing authorities do their roles and they are done properly. If you look at the recent audits they have just started doing on the operators with the ICO, they have agreed with industry what those audits will look like and what the definition and scope is going to be. The first actual audit was done last week on O2, so hopefully we will see the results of that come back. The one thing the Bill does very well is that it polices all the transparency in audit of what everybody is doing along that whole value chain.

Q157 Victoria Atkins: Mr Hughes, you have used the phrase "over-the-top providers" a lot. I may be the only person wondering this, but I suspect I am not: what do you mean by that?

Mark Hughes: The over-the-top providers I have referred to are companies that are running a communication service, such as WhatsApp, Snapchat, and Skype. They are examples of over-the-top service providers; they run a communications service using the underlying network providers that are here today.

Victoria Atkins: This is what I want to focus on. You have talked about how it would be more "elegant"—I think that was the word you used—for over-the-top providers to store this information, rather than you guys; sorry for being so informal. How on earth is law enforcement to know that one of the suspects that Ms Fernandes has referred to is on WhatsApp, Facebook or whatever unless they have that link in the middle, which is where you come in, signposting them to that application?

Mark Hughes: That is an excellent point. On signposting, we would have a role to play in saying, "We need to point you towards the company where you need to go to get the rest of the information about that customer", in a way they produce it and understand it. You make a good point about having to signpost the police in the first instance to what company has produced the communications service in question.

Victoria Atkins: If we just put that into the context of your evidence, you are not saying that your companies should play no role in this; you are worried about the details of decrypting and so on, but you understand that the Bill is phrased as it is to help law enforcement link a suspect to apps or services that they cannot know about unless you are involved in the middle.

Mark Hughes: Absolutely. This is about making sure that we do not blur the lines between traffic data and content by us having to open up all the packets of the data and then provide in an evidential way all the information to law enforcement.

Mr David Hanson: It is also about shifting the cost, is it not, from your perspective?

Mark Hughes: The Home Office has always had a policy of 100% cost recovery. They have assured us that this will continue. This is not an area that we make any money out of. We provide the very best service that we can to assist law enforcement.

Adrian Gorham: Another point worth making is that the customer of this is the police officer who wants the intelligence to allow him to make that arrest. If he believes that his target is using Facebook, the target may be using Facebook but it can use it on many different bearers. So it may use the O2 network; it can then go into a Costa Coffee and use a wi-fi network; it may then go somewhere else and use BT's wi-fi. It can use many different bearers, and you have to somehow get all that data from those different companies and put that all back together to show what that individual was doing on Facebook. If you go to Facebook and they have the encryption keys, they can tell you what is going on. They have all that data for that individual, so I do believe that it gives a much better service to the police to go to that one point of contact than try to go to each of the bearers that are carrying those communications.

Q158 Stuart C McDonald: You referred earlier to the process of setting up filter arrangements to get that communications data. What is your understanding about how request filters will work under this legislation, and would you have any concerns about the operation of request filters?

Simon Miller: We understand that the request filter is a mechanism by which large amounts of bulk or collateral data provided by us as communications service providers, as a consequence of requests made by law enforcement agencies, will be gradually—through a process of correlation and different data points—narrowed down to identify either a single subscriber or a smaller subset of users, and that this will be done by a trusted third party. The whole purpose of this request filter is to minimise the amount of unnecessary bulk data that will be handed over to law enforcement agencies.

We are all agreed as to the principle of this. There are a number of concerns, which Mr Gorham has alluded to, regarding the detail. The first is the fact that we would still continue to provide bulk data to a third party, and in so doing could be in breach of our duty of care under the Data Protection Act and the Privacy and Electronic Communications Regulations to our customers' data. The second is that we have absolutely no detail on what this trusted third party would look like, the form it would take, or the legal obligations that it would be under. As a minimum, we would simply expect that whatever operation the request filter undertook was done to the same standards, and was as secure, as our own arrangements.

Stuart C McDonald: So you have no idea who these third parties would be at all.

Simon Miller: Not yet, no.

Stuart C McDonald: What exactly is the filter? Who is responsible for putting that together, and would you have any ability to review what the filter was doing to your data?

Mark Hughes: I do not know who would be providing the service. I think it would be for the Home Office to select a vendor, to be able to build that situation. In principle, it is a good idea to be able to prevent lots of collateral intrusion. When you have really big, complex inquiries that you are running as a police officer, where you may need lots of data, the filter can be a way of reducing the collateral intrusion. The important thing here, as Mr Miller just said, is that whoever operates that has to operate it to the same standard in terms of the data that is being provided out of it, because this could fundamentally change the way network operators give evidence in court. Remember: we are potentially providing information into the filter. The operation, and what changes in the middle and what ends up on a police officer's desk from the query they have run is being provided by a person in the middle, a third party service—a vendor in this scenario. Again, we would need to make sure. It is going to take a lot of close collaboration to make sure this works well.

Stuart C McDonald: What sort of things would you want to see in the Bill so that you could have faith in that filtering process by the time you arrive in court to speak for the accuracy of the data you have provided?

Mark Hughes: We want direction and understanding on which parts of the evidential chain we would be expected to stand up in court and be cross-examined on, and whether, if the data had changed in the middle in some way, it would be the third party—for example, in this case, the vendor who is providing the service—that needed to attend court. I appreciate that these are sort of in the weeds, and they are quite technical things that we need to be thinking about, but essentially we are giving evidence in court on a day-to-day basis on mobile phone evidence, and we are worried about making sure that we can continue to do that with what is essentially a new piece of kit in the middle of the network.

Simon Miller: At the moment, this may be an issue for guidance, but these are discussions that the Home Office is yet to have with us, so we are dealing with an unknown. We are very keen that these discussions continue, and that these issues are bottomed out.

Stuart C McDonald: Any further thoughts?

Jonathan Grayling: Just to reiterate, the panel has said that the Bill places an obligation to provide security controls in relation to retained data, and those security controls are audited and will be audited. What is not in the Bill is that there are similar security controls for the request filter, and subsequently the customer data—my customer data that I am supplying to the filter. I would like to see the filter having the same security controls as the ones CSPs are compelled to provide in relation to retained data.

Q159 Matt Warman: Can you say a bit about what you understand by a technical capability notice, and what you understand by the Home Secretary being able to impose one at will?

Mark Hughes: Our understanding is that this is about the potential for equipment interference. Vodafone has three real concerns about this particular item. First, equipment interference could obligate a network operator to introduce, say, a backdoor or a way to launch some kind of attack against a particular target that may be using the network. You will probably not be surprised to hear that we have three concerns. First, we are worried about this representing a real diminution in trust in UK-based service providers, which may have to introduce backdoors on their network. In such a highly competitive marketplace, if you had to decide who to place your communication service providers with—a UK-based company that potentially has this obligation, or somebody else who does not—you may be really thinking about that.

Secondly, we are concerned about an obligation that may ask us to fundamentally reduce the level of security of our products or services, or our networks. We would be really concerned about introducing any reduction in the level of security of our products and services. Thirdly, we understand that, as it is written in the Bill, this may involve our people and our staff having to get involved in launching such attacks against targets across our network. We would be keen to make sure that that does not happen, and it is down to the law enforcement or the agencies to manage the workable provisions of that.

Matt Warman: Any other thoughts?

Jonathan Grayling: I would echo what Vodafone said there. With respect to the Bill itself, there are a number of aspects of control and oversight over those technical capability notices that we do welcome—significantly, the fact that the Home Secretary has an obligation to consult with the respective CSP prior to serving a technical capability notice on that CSP. That consultation has to take into account, among other things, proportionality, technical feasibility, the cost—which is significant for us—and the impact on our customers and our network.

Even after that consultation process, and a notice is served, there is still a mechanism whereby if the CSP is still unhappy or concerned with that notice, they can pass it back to the Home Secretary for further review and, again, the Home Secretary has an obligation then to consult with the Technical Advisory Board and the IPC, which we welcome. The key point here is that we need to ensure that each stage of that process is rigorously enforced, rather than a rubber-stamping process. If we have concerns about that, we want to have it demonstrated that the appropriate oversight and controls are being applied to that process.

Just one very quick, final point. My understanding of the Bill is that the IPC would have responsibility for the oversight of national security notices. I cannot find anything in the Bill that says that the IPC would have oversight for technical capability notices, so the question is why that might be the case.

Matt Warman: What do you think your customers would make of even an oversight arrangement that you were corporately happy with?

Jonathan Grayling: Customer trust is essential to our business, and the priority for us is to ensure that we provide a secure and resilient network. That is what our customers will expect. If there are any powers or any activity that is undertaken by the agencies in relation to equipment interference, whether that is proportionate and lawful is a matter for

Parliament and the agency itself, but EE would not accept it if those activities had any impact on the security of our customers' data or the resiliency of our networks.

Q160 Matt Warman: Moving on to the IPC that you mentioned, do you think that the level of engagement that is outlined in the Bill between you and the IPC is sufficient to maintain that level of security and trust?

Simon Miller: The levels of engagement envisaged are broadly similar to those that we have currently with existing authorities. Interject, gentlemen, if I am talking out of turn, but those levels are appropriate to the subjects concerned. The issue for us has always been that they are broadly uncoordinated, and as a consequence of that there are business impacts. In particular, at the margins, there are jurisdictional overlaps with different authorities talking to the same subject with different voices. It therefore follows that we are fully in favour of the creation of a single body, the IPC, that will have all these powers of oversight, and it will rest in that one body. The simple fact of the matter is that the current practice of having separate bodies with these different functions is, for us, broadly cumbersome, open to misinterpretation and misunderstanding, and time-consuming.

As for the actual level of engagement, this would be a new body. We would fully expect levels of engagement to ramp up as that body beds in and to have to adapt to new personnel and new ways of working. It is probably worth saying at this point that the relationship that we all have with IOCCO is an exemplar. If the IPC were to look at the ways of working exhibited by the existing authorities, it should look to IOCCO as a model of best practice, and we would very much like to see those practices demonstrated around building strong, coherent stakeholder relations, early engagement and demonstrating sector expertise continue.

Matt Warman: Broadly, it sounds as though you are looking forward to the changes that are coming, rather than dreading them.

Simon Miller: Absolutely.

Adrian Gorham: It might also be useful if there is an express right for the operators whereby if we have an issue or a complaint about one of the LEAs or the police we can go directly to the IPC to report that. That is not to say that there have been any issues previously with them, but it is worth having in the legislation so that we have that channel should we want to use it in the future.

Q161 Lord Strasburger: Would you agree that equipment interference is one of the most technically complex and risky activities that we are looking at in this Bill, and do you think there is a case for having some sort of technical oversight as to what you are being asked to do from a third party, as well as having judicial oversight?

Jonathan Grayling: In the Bill, there is a mechanism to refer to the Technical Advisory Board, and we would expect that Technical Advisory Board to provide that independent oversight. Because of the additional obligations in the Bill, there should be a review of the TAB to ensure that it is structured appropriately and has the appropriate individuals around the table with the appropriate knowledge. That is necessary.

Lord Strasburger: These are very specific skills, are they not?

Jonathan Grayling: They are.

The Chairman: Thank you very much indeed. We have now come to the end of the formal session.