CORRECTED TRANSCRIPT OF ORAL EVIDENCE To be published as HC 479-ix

---

HOUSE OF LORDS

HOUSE OF COMMONS

ORAL EVIDENCE

TAKEN BEFORE THE

JOINT COMMITTEE ON THE DRAFT COMMUNICATIONS DATA BILL

DRAFT COMMUNICATIONS DATA BILL

TUESDAY 16 OCTOBER 2012

3.15 pm

Witnesses: Sir Paul Kennedy and Joanna Cavan

Christopher Graham

Evidence heard in Public Questions 660 - 713

USE OF THE TRANSCRIPT

1. This is a corrected transcript of evidence taken in public and reported to the House. The transcript has been placed on the internet on the authority of the Committee, and copies have been made available by the Vote Office for the use of Members and others.

2. The transcript is an approved formal record of these proceedings. It will be printed in due course.

Members present

Lord Blencathra (Chairman)
Lord Armstrong of Ilminster
Baroness Cohen of Pimlico
Lord Faulks
Lord Jones
Lord Strasburger
Mr Nicholas Brown
Michael Ellis
Dr Julian Huppert
Stephen Mosley
David Wright

_____

Examination of Witnesses

Sir Paul Kennedy, Interception of Communications Commissioner, Interception of Communications Commission, and **Joanna Cavan**, Chief Inspector, Interception of Communications Commission

Q660 The Chairman: Welcome to our public evidence sessions. Welcome to Sir Paul and your colleague. I am sorry you were kept waiting. We were just about ready to start at 3 pm when a vote occurred in the Commons. We are likely to be interrupted throughout the day with votes in the Commons and Lords as well. I am sorry about that but that is the price we pay for living in our wonderful democracy. Before we start with questions, Sir Paul, could I ask you to briefly introduce both of yourselves for the record?

Sir Paul Kennedy: I am the Interception of Communications Commissioner, and have been so since 2006, so I have done something over six years in that office. My colleague is the chief inspector, who works under me with a team of five inspectors under her, and perhaps I can explain—if you permit me to do so—the way in which our work divides.

I in fact have two parts to my role. One is the oversight of interception, and I am sure that you are all sufficiently familiar now to know the difference between interception and data. Interception is that part of the activity that is covered by chapter 1 of part 1 of RIPA. I do that myself, so that my function is to check that the Secretary of State who grants a warrant has done so on grounds that are sustainable. It is an auditing function carried out after the event and I do it. I also have an oversight role in relation to data. Data of course is not the content, it is the context—if I can put it that way—of any communication.

As you know, there are a large number of occasions when data is obtained, and it would be physically impossible for me to do them all anyway. So that side of my functioning, in other words the oversight of data, is carried out on my behalf by Ms Cavan and her team of inspectors, and that is how our functions relate. In the early days of my activity I did do a couple of inspections on her side of the fence so that I understood what was going on, but in reality I do not normally see anything other than the reports that her team produces, and they are incorporated into my annual report. I hope that is helpful and explains our two different functions.

The Chairman: It is very helpful, Sir Paul, and thank you for that opening statement. Could I ask Lord Armstrong to ask the first question, please?

Q661 Lord Armstrong of Ilminster: Sir Paul, you said in your written evidence that a strong case has been made that without the draft Bill there will be a declining capability. I wondered if you could tell us what was the evidence, in more detail, that persuaded you to take that view.

Sir Paul Kennedy: It is quite difficult to give you specific examples without crossing a line that I could not do in a public forum. I think you already have the evidence from others that over the last few years what has happened is that there has been a

decreasing amount of the information that an investigator—if I can put it that way—either on the counterterrorism side or on the domestic policing side, requires being available. It has never been available 100%. That is a myth. You have not always been able to get everything you wanted, but the amount that you cannot get has increased and it has now reached the position where it is said about 75% of what you need you can obtain, and the figure is falling, and within a couple of years it will be down to about two-thirds of what you need.

If you think of it that coincides with what we all know from our personal experience. When I started to do this job—only six years ago—people who were engaged in illicit activity communicated probably by mobile phone. They now communicate much more frequently by internet protocol, and they can do so without leaving anything like as great as a footprint and sometimes no footprint at all, and it is in order to meet that increasing risk that, it seems to me, the main thrust of this Bill is an essential step for Parliament to take. Does that answer?

Lord Armstrong of Ilminster: Yes, thank you very much.

Q662 Lord Jones: Sir Paul, I am to ask my question on behalf of the Chairman and the Committee.

Sir Paul Kennedy: Yes.

Lord Jones: It is like All Gaul: it is in three parts. May I proceed? When your inspectors randomly sample the applications put forward by large users of communications data, what percentage of applications do they inspect? Then, how many of the 494,000 requests made in 2011 did the IOCC team inspect? And thirdly, are you satisfied random sampling gives a reliable picture of each authority?

Sir Paul Kennedy: Can I first of all put aside the small users because, not surprisingly, when my inspectors go to a small user who has made seven

applications—and that would be quite a lot sometimes—for data over the last two years, they inspect them all, so there is no question there of any type of sampling. That accounts for a percentage, but a small percentage, of the total figure you have just been talking about.

The remainder, about 488,505, are the big users. Different considerations apply, and I think it is important to have this in mind also. Someone like the Metropolitan Police have a trained team of what, in the jargon are called SPOCs—single point of contact officers—and therefore you are dealing with a sophisticated arrangement. By contrast, the small users, for example the local authority, have not done one for two years and they have quite a difficulty in knowing how to do it right, so one starts from that perspective.

The next thing that I would like to stress is that there is a difference between requests, which is the 488,500-odd, and applications. That is not easy to hold on to, to begin with. In order to acquire data you must make an application. The application may immediately generate several requests; different telephone numbers, if I can put it that way. Because the statistics are not complete across the board, we do not at the moment have easily accessible the numbers of applications, but an inquiry was done by Ms Cavan to try and see what the relationship was. It was not a particularly prolonged inquiry. It was only conducted over a limited period, but it looks as though you might say that each application gives rise to at least two requests so you need to bring the numbers down[1]. If you do that, and then you look at the number of applications that were inspected by the team, the answer comes out to, in round figures, about 10%. That answers the first part of the question satisfactorily, I hope?

Lord Jones: Thank you, Sir Paul.

[1] Sir Paul Kennedy clarified the inquiry revealed an average of 3 requests per application.

Sir Paul Kennedy: That seems to us to be a reasonably sensible level. If you think of it in terms of auditing, perhaps in the accountancy world it is a reasonable level at which to operate. Now does that give one a fair picture?

There are other riders we have to attach to this. The first is that an application itself, when you are looking at it, may disclose an error of procedure—not often, happily, but it does. If that happens in the context, for instance, of a large police force, the next question of the inspector will be, “Have you been doing this all of the time? Let us see the other ones”. So there is the spillover effect. So the actual figure that has been inspected is not, as it were, tunnel vision; you will find the bits to the side as you go along. Because you are there for a day or two days doing an inspection, you get a pretty good feel of whether this team is working well or is not working well, and it is not surprising that when you go back 18 months later—and I have been in post long enough to see the reports in relation to all of this—normally speaking, those who have it right will go on being able to get it right, unless, for example, there has been a change of staff or something of that kind, or the computer system has been playing up or something of that kind. So I think the answer is—if I have remembered all the legs of the question—so far as the first, put in bald figures: about 10%. Do we get a good feel as to whether or not the system is working well? Yes, I think we do, but only because you are there for quite a long time and systemic errors that are discovered hopefully are able to be corrected at the time when the investigation is taking place.

Lord Jones: I am grateful, and—

Sir Paul Kennedy: Do tell me if I have not covered everything.

Q663 Lord Jones: Colleagues will I am sure. But the annual report is helpful, and I see you have the chief inspector and then five inspectors.

Sir Paul Kennedy: Yes.

Lord Jones: Are you able to tell us how you acquire such people? What kind of people are they? How long are they with you?

Sir Paul Kennedy: Happily, they do not change jobs very often, which I am extremely grateful for, because they acquire expertise. Give your CV; can I ask her to give her CV?

Joanna Cavan: I have worked for the commissioner and the previous commissioner for nearly eight years now, and we do have quite a consistent team who have been supporting the commissioner for some time. I came from a private company where I worked as an independent expert witness in forensic telecommunications, and prior to that I worked for a police force. The majority—well, it is a split actually, half of my inspectors come from a police background where they are senior retired police officers and the others are civil servants, so we have a mixture of backgrounds.

Sir Paul Kennedy: The civil servant ones are mostly Customs.

Lord Jones: Would you take part in the selection of the inspectors?

Sir Paul Kennedy: Yes. I took part in the promotion of this one because she succeeded her predecessor, and I think I took part in the last appointment we did too, so yes, I do. We advertise within a fairly confined area. Obviously we do not go to the national press, I do not think, on this but we advertise in Civil Service periodicals and police periodicals and so forth, when a vacancy occurs. You need to have—and I have seen this in other walks of life—people who have a certain degree of competence obviously, but who are available to do this kind of work usually because they have ceased to do something else. In reality, senior police officers or senior Customs officers who are just on the point of retirement are the sort of people who tend to be interested in this kind of work. From our point of view, it seems to me that

they are useful people to have on board because very often they have used material at the other end and they have had experience of how the systems do work or ought to work, so they need less training and are more alive to the work we are doing than they would be if they came cold from the public.

Q664 Lord Jones: Lastly from me, Sir Paul, may I ask you: how often does somebody like you see the Home Secretary, and have you seen the Home Secretary—this one—to discuss this draft Bill?

Sir Paul Kennedy: No, is the answer to the second question. I see the Home Secretary normally once a year and—this is my other role, in relation to the warrant-signing Secretaries of State—I see all the warrant-signing Secretaries of State on an annual basis. If I need to see any of them for a specific purpose, then I ask to see them but, in fact, normally I see them on an annual basis.

Lord Jones: Thank you.

Q665 Lord Strasburger: I would just like to return to the first question for a moment. I did not get a chance initially. You stated that there is a capability gap of 25%, rising to 35%. Is that your own assessment or is that one that you have heard elsewhere?

Sir Paul Kennedy: No. I do not have the facilities to give my own assessment in that way, but I know from what I hear. In all the agencies I visit—and I do visit them quite regularly in the course of my work—they tell me, “We weren’t able to progress that any further because we cannot get that data”, and that is an increasing problem for all of them. So I do not measure it. I cannot measure it.

Lord Strasburger: The figures of 25% to 35%; you were repeating what—

Sir Paul Kennedy: What you see in the papers you have yourselves.

Lord Strasburger: —I presume the Home Office said?

Sir Paul Kennedy: Yes, who gather it from the agencies.

Lord Strasburger: Thank you.

Q666 Mr Brown: Have you tested the labour market more broadly for senior operating staff, and are you not worried—I understand your reasons and I think you have put them very well—that you might be drawing your staff from too narrow a base and that there might be a breadth of experience that you are not drawing on?

Sir Paul Kennedy: We have not tested the labour market more widely, no. On the other hand, I am not troubled about the base. If I can put it to you this way, if you saw some of the reports they produce when they are being critical of a police force, and they themselves were police officers, you would not have any worries. It is quite clear that they understand exactly what they are there to do.

Mr Brown: If it is any comfort to you, the police said something similar when they were here.

Q667 The Chairman: Sir Paul, can I just follow up as well on your first answer to Lord Armstrong and Lord Strasburger, on the capability gap? You have said you have seen in your six years the change from mobile phones to other means of communication. We have also heard a lot of evidence from others before this Committee to say, "If you looked at my mobile phone in the year 2000 you would get fairly bare bits of information from it. If you look at a modern mobile phone these days you will get thousands of extra bits of information, of websites and so on", so the overall amount of information has gone up exponentially. How does that relate to the so-called gap?

Sir Paul Kennedy: I agree with what you, my Lord Chairman, have just put to me, that the amount of information capable of being taken is greater. On the other hand, if a mobile phone is serviced by a provider who has no personal business to keep the

records, you cannot get anything because you are not getting into it at all. That is the real problem, that for very understandable reasons six years ago every provider, I think I am right in saying, in the marketplace had a business reason for keeping their own records, and it was those records, particularly in retrospect, that one was able to tap. If you were doing an inquiry in relation to a murder, you would be able to look for the records of the mobile phone that was found in the possession of the suspect, and what they had been doing at the critical times. Now the situation has moved on to a position where that provider simply says, “I have no records at all. I had no business reason to keep them. He pays me so much because he buys the phone and he buys a certain amount of time, or he has a contract that I do not have to keep any records of”, and the inquiry is at an end. If the provider is abroad—and this is an increasingly international market—the problem then is of the same dimensions.

The Chairman: I understand.

Q668 Dr Huppert: Sir Paul, how do your investigators judge what is a justifiable level of intrusion for communications data? When you are looking at the records, what are you looking for? How much information can you get to assure yourself?

Sir Paul Kennedy: What is a justifiable level of intrusion?

Dr Huppert: Yes.

Sir Paul Kennedy: I think you have to look at it on a case-by-case basis. There is no way in which you can say some formula will work across the field, but you look at necessity and proportionality in relation to any given application. On the ground—I think I can say hand on heart—it is not that difficult when I see what is in the reports and, performing my other role, I see what is put to the Secretary of State in an application for a warrant. It is perfectly easy to see. There are not that many that are near the borderline. There are a few.

Dr Huppert: So you look at the reports of 50,000 assessments and you think that they are all relatively easy to tell? That is your—

Sir Paul Kennedy: No, I am looking at the report of the ones that have been inspected by my inspectorate.

Dr Huppert: Which is a 10th of the whole data?

Sir Paul Kennedy: Yes. They are recording what they find. They are normally more addressing the procedure being properly operated. They will be looking at the individual cases. The report will be dealing with the satisfactory nature of the procedure. Of course, if there is an inappropriate application then it would come into the report. I do not pretend that the report is a reflection of every piece of paper they have looked at. Well, I take that back. They do not look at pieces of paper at all. This is all electronic. But of every application they have looked at, it will only highlight occasional ones, I agree.

Dr Huppert: According to your last report, your inspectors found 100 errors, or was it 99?

Sir Paul Kennedy: Yes, 99.

Dr Huppert: So there are some errors that are reported to your office automatically, but 99 you found by looking at a 10th of the data?

Sir Paul Kennedy: In fact, 77 of them, I think I am right, were local authority ones, and as we inspect 100% of the local authority ones you can take it those are all the local authority ones. So it is only the remaining 22 that come from the rest of the field, but 22 is 22 too many, I do not disagree. Very often, or nearly always, they are procedural errors. The sort of thing that we have found—I think I am right in saying off the top of my head—is the wrong level of persons signing the authority. In the police it is quite easy because an identified rank is established, but in, for example,

local authorities there was no necessarily equivalent rank and it was signed at the wrong level. That is an error and it should not have happened, but it is not one that causes me to feel great anxiety.

Dr Huppert: But it would presumably mean that the evidence could not be used in a court? Certainly, if the wrong rank of police officer gives an instruction, whether it has to be an inspector or higher and it is somebody lower, that is not a valid thing in court, so presumably any of those glitches would mean that that evidence could not be used in a court, is that right?

Sir Paul Kennedy: It may or may not be right. It depends on the context. It is a ground for raising it in court. On what the judicial ruling would be as to the admissibility of the evidence, I would prefer to be sitting as a judge before I answer the question.

Q669 Dr Huppert: There are different rules for different data types. We have talked about content as one thing, use, traffic and subscribers—

Sir Paul Kennedy: That is a very important aspect of what you have just raised a moment ago, that the vast majority of applications—and I am sure you will appreciate this already in relation to data—are what one might call telephone book applications. They are to find out who was associated with this number. For many of the bodies who have powers, they only have power to get that kind of information, which is subscriber data.

Dr Huppert: Sir Paul, I think we are familiar with the breakdown but the definition, which I am sure you are familiar with, for subscriber data is, “information (other than traffic data or use data) held or obtained by a person providing a telecommunications service about those to whom the service is provided by that person”. So presumably that means if I have an e-mail account that is organised by the University of

Cambridge, as in fact I do, then subscriber data is not just the reverse directory you look up, which you have talked about, it would also include any information that the University of Cambridge holds on me, is that correct?

Sir Paul Kennedy: On the definition, it is. I cannot remember it ever actually being, in practice, a situation I have looked at, but yes.

Dr Huppert: So if the university held my medical records from when I was a student, which again it does, that would count as subscriber data according to what this says, because it would be information held or obtained by a person providing a telecommunication service about me?

Sir Paul Kennedy: I would like to think about that one. I am not sure.

Dr Huppert: This has been raised to us as a very serious concern because it is very broadly written. If you could write back to us that might be helpful. Subscriber data in the current Bill is page 63—

Sir Paul Kennedy: In the current—sorry?

Dr Huppert: In the current draft it is page 63, section 5. It is very broadly written and allows far more than the directory look-ups I think you are identifying.

Sir Paul Kennedy: Page 65?

Dr Huppert: Page 63, but if you want to write back to us I think that might be more useful than—

Sir Paul Kennedy: Sorry?

Dr Huppert: If you want to write to us about that I think that might be more useful than an immediate response.

Sir Paul Kennedy: As I understand it, what you are seeking is whether I am satisfied that the subscriber data is sufficiently narrowly defined. Have you an alternative to put?

Dr Huppert: One could define it in some sense as a reverse directory look-up whereas this allows any information held to count as subscriber data. If you look at the information that Facebook would hold on me, that Google would hold on me, it is very significant, and it is not at all clear here what that definition is. I hope that you are clear when you are doing inspections because, as you say, subscriber data is a lower level of authorisation.

Sir Paul Kennedy: Oh yes. In fact, that is what it is in reality. The width of the definition is not a point that has ever actually been a materiality so far that I can remember.

Q670 Dr Huppert: Can I then move on, because one of the things we have had a lot of concern about is how broad some of the investigations are? There is a big difference between a police officer asking for information on a particular phone and asking for very general information—that may be a cell dump, it may be collecting data from a mobile phone provider for every client for the last two weeks or something like that.

Sir Paul Kennedy: Every?

Dr Huppert: Every user, where were they in the last two weeks. One can imagine something very, very broad. Do you do anything systematically—

Sir Paul Kennedy: I do not see how that would possibly satisfy any of the existing tests. It could not be proportional.

Dr Huppert: I would tend to agree, Sir Paul, but reality does not always fit with what is actually proportional. But do you do anything to systematically look for phishing attempts?

Sir Paul Kennedy: Yes.

Dr Huppert: Do make sure they are individually checked, and how do you do that if you are only looking at a sample of requests?

Sir Paul Kennedy: No, that is probably something that I ought to go into a little bit more deeply. The nature of an inspection does focus on various aspects and, for instance, if there is a cell dump they would be looked at automatically as part of the inspection. If I can break it down, the way in which the inspections operate is you start with a random sample from the record of whichever police force it is. You then take a random sample of the data that that police force has asked for from the service providers, so that you get a back check. If I can put it this way, you go to Vodafone and you say, "How many requests have you had? Give us the number in the last 12 months from Cambridgeshire", and we will select a few of those. Then when you go to Cambridgeshire you say, "Produce the files in relation to those", so that is a back check.

Q671 David Wright: On that point, would you take a specific incident, outside of your random sampling, and investigate that incident? For example, a specific terrorist incident within the UK, would you actually look at that particular incident and the communications data used on it?

Sir Paul Kennedy: I think in reality almost certainly, because if you inspected that police force you would be looking at a big incident of that kind. Life is like that. They would want to show it to you and you would want to look at it, so yes. In every inspection, or pretty well every inspection I can think of—and we are rather focusing on police forces—they do produce examples of a particular operation and how the acquisition of data worked in relation to that operation. So, yes, they come very often as an appendix to the report on that police force.

David Wright: Earlier you said that you would use your judgment as to what was reasonable because each case was almost standalone in its conduct.

Sir Paul Kennedy: The person who uses the judgment in the first instance is not me. We are doing it retrospectively.

David Wright: Help us to understand how that process works then.

Sir Paul Kennedy: What you do is you look at the information you have obtained and decide whether, in those circumstances, it was reasonable to use the statutory powers—it was necessary and proportionate to do so. Given a particular set of facts, I do not think it is a difficult operation.

Q672 The Chairman: Sir Paul, can I move on to the possible extension of your powers if this draft Bill becomes law?

Sir Paul Kennedy: Yes.

The Chairman: In your written evidence you state you do not know how much extra work it will entail and how often you will need to inspect the CSPs, how many CSPs will be affected by the draft Bill, and so on. Are you concerned that at this stage you have not been given enough information by the Home Office about the potential extension of your responsibilities?

Sir Paul Kennedy: May I say, first of all, this is in fact not going to be me because my term of office ends at the end of this calendar year, but I will pretend that it is me.

The Chairman: Well, the office of commissioner.

Sir Paul Kennedy: The office of commissioner goes on. I am in no way critical of the amount of information that we have so far been receiving, because the Home Office has kept us in touch with these matters as they have developed. I think it is very much an area where we will have to learn by experience and I have had specific assurances that what we need we will have. So far as the first of the additional duties

are concerned, I think that is probably one that can be dealt with by the chief inspector and her team of inspectors. So far as the second part of what is envisaged is concerned, that is the filtering side of the operation, I think—and I am only guessing here because we have not yet got anything in place against which you can run the tests—that will require a degree of expertise that at the moment we do not have in-house. For that purpose it may well be necessary to recruit someone with an IT background, either on a full-time or a part-time or a consultancy basis, to discharge the obligation that is placed upon the commissioner by the Bill if it becomes law. At the moment to say we ought to be going to the market for it, I think, is premature. I think until we see exactly what is required it is too early to do so. Furthermore, the way in which the Bill operates, as I understand it, is that an order would be made by the Secretary of State in relation to a particular provider. It would be at that stage that one would be looking about the operation of the Bill as a whole. Therefore, I think there is time, and it would be better if the time was used and the recruitment when it takes place was focused and appropriate. So I am satisfied we are being kept up to date, yes. Are we going to need more help? Yes.

The Chairman: I should have asked Mr Ellis to come in at that point, and I intervened by mistake. Mr Ellis, if you wish to continue in this line?

Q673 Michael Ellis: Just briefly, Lord Blencathra. Sir Paul, as far as the whole extension of your powers is concerned, do you have any idea as to when you might get these details from the Home Office?

Sir Paul Kennedy: In one sense, no, but I hope—

Michael Ellis: You are quite relaxed about it, though?

Sir Paul Kennedy: I am relaxed about it because I do not think we should try and jump the gun.

Michael Ellis: No.

Sir Paul Kennedy: Something has to be done when we have the information, of course.

Michael Ellis: How much time will you need to recruit new staff? Do you anticipate needing new staff?

Sir Paul Kennedy: Probably not in large numbers, but probably the answer is yes. How much time do you need? It depends on the answer to the previous question, does it not? If we are dealing with people who are technically qualified, are we going to recruit them on a full-time basis or are we going to recruit them, for example, on a consultancy basis? If we need to get somebody on a full-time basis, three to six months.

Michael Ellis: Do you engage your current staff on a full-time basis?

Sir Paul Kennedy: Yes.

Michael Ellis: Are you confident that your current staff have the expertise required to take on the new responsibilities?

Sir Paul Kennedy: I think I have already answered that. In relation to the first section, from what I know of the Bill so far, yes. In relation to the filtering section, not necessarily. Probably not. I would not have, so I do not expect them to have.

Michael Ellis: You would have an idea of where to find them?

Sir Paul Kennedy: I think when I see what the filter involves I might have to take advice from people technically qualified within the Home Office as to where we should be looking. But my present impression is that which I have already indicated, that people who have IT qualifications are probably the ones we will be looking at but within that very broad field, a precise area to target, I do not know.

Michael Ellis: They will be vetted individuals?

Sir Paul Kennedy: They will have to be, unless they are already in the service. This is how sometimes one is lucky enough to recruit people who already have been vetted. But you are quite right, that is another timescale.

Michael Ellis: Do you currently ever see applications for communications data made by public authorities?

Sir Paul Kennedy: Yes.

Michael Ellis: Is that through the mutual legal assistance process?

Sir Paul Kennedy: No. We do not involve the mutual legal assistance process at all. That is controlled by the courts and we have had no hand in that at all.

Michael Ellis: Do you have any observations about how that works?

Sir Paul Kennedy: It is slow.

Michael Ellis: Slow—does that mean inefficient?

Sir Paul Kennedy: I think I know as much as you do, in the sense that I see what the timescale is in relation to matters that have gone through that route. I am not prepared to say it is inefficient. It would be wholly unsatisfactory to make a criticism of that kind without having been involved in investigating it properly.

Michael Ellis: So you are generally confident, though, that when furnished with the information that you require, your successor will be able to deal with the issues appertaining to staff and facilities appropriately?

Sir Paul Kennedy: Yes, I think so. It required an assurance, which I have had from the Home Office, that essentially if I or my successor goes and says I need another member of staff they will have it. That assurance has been given.

Michael Ellis: In your six years, have you made such requests previously?

Sir Paul Kennedy: For increases in staff?

Michael Ellis: Yes, or equipment or facilities or anything along those lines. You have?

Sir Paul Kennedy: Not to a great extent, but to a limited extent, yes.

Michael Ellis: You have not met with any obstruction or difficulties?

Sir Paul Kennedy: No.

Q674 Michael Ellis: So, just to take a step back if I may, just on the need for this draft Bill, you are coming up to the end of your distinguished term in this position. I think you say you finish at the end of the calendar year, is that right, Sir Paul?

Sir Paul Kennedy: Yes.

Michael Ellis: If one was to invite you to make a brief appraisal of your six years in the position and how you see things going forward perhaps in the next six years, are you satisfied, in all the circumstances, that this is a necessary measure that is both proportionate and also meets the challenge presented by criminals and terrorists and other wrongdoers going forward?

Sir Paul Kennedy: Absolutely, is the short answer. I have no reason to doubt—indeed, this is where we began—the figures that I have been given as to the extent to which the ability to obtain information has been contracting. I regard that as potentially very dangerous, and it means that we are unsighted in a section of the market, and we are in a world that is still extremely volatile. It seems to me that, against that background, what is now being sought is not to increase the amount of information available in the public domain principally, it is to require service providers to retain certain information that can only be accessed in a proper way—that is to say, when it is shown to be necessary and proportionate to access it. Then it can be used not only for the purposes of securing convictions—one tends to forget because that is the side we can talk about—but also by the intelligence services for disruption.

Disruption is a hugely important part of the safety that we all enjoy. A lot of it is never even mentioned but, in fact, if they lose the capacity in that direction, and you lose the capacity to detect crimes that have been committed, to the extent of which could be something in the region of 20%—one in five of the pieces of information you want—that is very serious and we should not be doing that, either for our own safety or the safety of our children.

Q675 Lord Strasburger: Sir Paul, this draft Bill will add a very large amount of data, on top of the data that is currently covered by RIPA, and therefore this Committee is concerned to be comfortable that the auditing of RIPA is going well and, secondly, we are concerned to know how well the public authorities are complying with the law. I have read your 2011 report very carefully. It is quite long on enthusiasm for the benefits of communications data but it is quite short on the details of your inspections. As an example, on page 33 and page 44 there are two graphics that show the level of compliance for two groups of public authorities. You have grouped them into good, satisfactory and poor, but I have no idea how good the public authority has to be to be good. What percentage of compliance does a public authority need to achieve to reach your category of “good”, and equally for “satisfactory” and “poor”?

Sir Paul Kennedy: We tried to make an overall evaluation of the reports in the way we put the message across. If you read the remainder of the text around the graph, you realise how they have come into existence. The vast majority of police forces and law enforcement agencies had fully implemented the previous recommendations. When the inspectors go they make recommendations, and if they implement previous recommendations then you get to a situation where their performance is of a level that you expect to be good. If at the time of inspection you find that they are not

complying with the Act in certain respects, it may be a minor error, it may be all right but not very good, it may be simply awful, and we have tried to make those distinctions in those bar charts. I do not know how much more we could do that would be of help, but if we could we will certainly try.

Lord Strasburger: In order to get into your "good" category, does that mean 100% of requests were compliant, for example?

Sir Paul Kennedy: Yes, in most cases. Yes. The 72% is not a 72% good. It is 72% saying you are an efficient authority.

Lord Strasburger: Yes, but what does "good" mean? I am still trying to find out what "good" means. Is it 100% compliant, 80%, 90%? I am trying to get a handle on how many—

Sir Paul Kennedy: It means that if you go to a police force and there is very little, if anything, wrong with the way in which they are using their statutory powers you class them as "good".

Lord Strasburger: What is the level for "satisfactory" then?

Sir Paul Kennedy: The level of "satisfactory" is not as good. It is the next level down. It is that they are not as good as that. They in fact have some errors, but overall they are doing it quite well—satisfactory.

Lord Strasburger: How many errors is "satisfactory"?

Sir Paul Kennedy: If you ask me in relation to a particular police force I will go and look it up, but I am sorry—this is marking all over the world. It is like academic marking. You have good ones and satisfactory ones and poor ones.

Lord Strasburger: In order to get a grade in my GCSEs, I will know that to get grade A I have to achieve 72%?

Sir Paul Kennedy: Yes.

Lord Strasburger: What does a public authority have to achieve to become good or satisfactory or how bad does it have to be to be poor?

Sir Paul Kennedy: I am sorry, but if there are a lot of errors then it is poor. If there are only one or two errors, it depends on the quality of the error. If the error is significant, and there are two or three of them then they may be poor although there are only two or three errors. If there are two or three errors but they are not very serious errors they may still be satisfactory. I cannot do any better than that without referring to a particular report.

Lord Strasburger: You are telling me that it is a totally subjective judgment?

Sir Paul Kennedy: It is not a subjective judgment. It is a judgment made on the basis of carefully prepared reports, and I suspect you would support it if you read the report.

Lord Strasburger: I cannot do that.

Joanna Cavan: Perhaps, Lord Chairman, if I could possibly come in here and just add some context? The “good”, “satisfactory” and “poor” ratings come out of the recommendations, and this year for the first year we have disclosed the traffic light system that we use for recommendations. The recommendations are made across very distinct areas. We have set inspection baselines, so when you talked about “in your GCSEs you have to hit certain marks in certain areas”, we have a very structured inspection baseline document that covers the application process, the authorisation process, the urgent oral process, the content of authorisations and notices that goes to the service providers, on the quality of those. We inspect a number of baselines that come directly from the acting code of practice, and we mark the public authority against those baselines. If we then make a recommendation against one of those baselines, if it is a very serious compliance issue that has

caused breaches or potentially data has not been acquired in accordance with the law, that will be given a red compliance recommendation. It is very unlikely then that that public authority would get a good grading overall if they have some red serious compliance recommendations.

What we wanted is, if we give a public authority 13 recommendations, it was very difficult for them to decide which ones to hit first, which ones were perhaps more serious compliance issues that they needed to address, so that is why we introduced the traffic light system that shows the severity of each recommendation against each baseline. Then a chief officer is able to say, “Okay, in this area we have really serious poor compliance. We have red recommendations so we need to address those”. So once we see the number of recommendations, the colours of those recommendations, which represent how serious the compliance is, we will then use those quantitative results to move them into either a “good”, a “satisfactory” or a “poor” category. Those who have ended up with a “good” overall will have mainly green recommendations that are more around efficiency and effectiveness, whereas those who have been given a “poor” rating will have recommendations around the red category, which are serious compliance issues. I hope that helps.

Lord Strasburger: So the ratings are about process—how well they are applying the process? They do not give me any indication of how many times public authorities are not complying with the procedures or are making requests that are not compliant.

Joanna Cavan: They will include that, because if a public authority has made a request that is not compliant, that will automatically be a red compliance issue.

Lord Strasburger: How can I find out how often this happens?

Joanna Cavan: We will report on the serious cases in the annual report. It is very difficult to report on all cases we find because of sub judice, so we cannot report on

absolutely everything openly. But they will be mentioned in the report where we have found serious non-compliance issues.

Lord Strasburger: I am just after statistics, that is all, I am not after the details.

The Chairman: Would you possibly be able to send those to us?

Joanna Cavan: I could certainly have a look at that for you. Of course.

The Chairman: Yes, please. That would be helpful.

Q676 Stephen Mosley: When you are looking at the compliance do you look at the technical systems used by the public authorities, or do you rely on the paperwork that you are supplied and the recommendations that you are supplied from those authorities?

Sir Paul Kennedy: The answer is there is no paper. The answer is you look at the base material.

Stephen Mosley: So you go in there and you look at their technical systems and make a decision based on that for a public authority.

Sir Paul Kennedy: Yes.

Stephen Mosley: What about with a CSP?

Sir Paul Kennedy: Sorry?

Stephen Mosley: What happens with a communications service provider that might not be a public body?

Sir Paul Kennedy: I do not have any role in relation to communications service providers. I do see them and I visit them, but I do not have a statutory obligation to do anything with them, other than talk to them and see that they are getting the service they need from the other end. I cannot go to them and say, “Produce to me your records”. I have no statutory warrant to do so. In this Bill, there is a certain role in relation to communications service providers. There was not previously. But, for what

it is worth, I have always gone not to all of them but to the large providers, in order to talk to them about what they do and to make sure that the relationship they have with, for example, agencies is a satisfactory one.

Stephen Mosley: Would you have a role at verifying the interception and communications data logging equipment that has been put on the CSPs' networks?

Sir Paul Kennedy: As I understand it, that is part of what would now be envisaged, yes. We will know how this will work out on the ground when we know more of the technicalities.

Q677 Stephen Mosley: Going back to the public bodies, you say you currently have the right to go in there and verify their systems. From some of the evidence we have seen—and I know Big Brother Watch says this—people say that you might have the power to do it but there does not seem to be anything in your reports to say that you have actually been in and looked at the systems themselves, rather than relying on the evidence that they supply you. Have you ever used those powers to go in and look at their systems?

Sir Paul Kennedy: Yes.

Joanna Cavan: We do conduct the inspections on the systems, so nothing is printed out for us. We have log-ins to that public authority system and we conduct the inspections on the system. So we do a full audit trail and the action is taken on that system. We would not be able to do it on paper because we would not be able to see the audit trail, as the process works electronically, so if you were not examining it on the system it would not be robust enough.

Stephen Mosley: Moving to the new system, when you have the rights to do that with the CSPs as well, do you think those CSPs would be happy to allow you to have that authority to do it on their networks?

Sir Paul Kennedy: The degree of co-operation we have always had from the CSPs is very high. One of the basic factors is that in this country we pay the CSPs for their co-operation. I am not saying they make a great deal of money out of it but they do not lose money out of it and we do get very good co-operation. I have no reason to doubt that if this Bill were to become law that would continue. As I understand it—and it is quite important to make this point—the purpose of those who wish to see this Bill become law is not to use the powers enshrined in it, except when they have to. They want to obtain most of the material that they need to have, by means of co-operation. I think that the past suggests that that will be possible provided there is in place a statutory formula to be used if the co-operation is not forthcoming. That is why I think this Bill is very necessary.

The Chairman: Thank you very much, Sir Paul.

Q678 Baroness Cohen of Pimlico: I would like to ask you about the warrant system in relation to local authorities. It is quite a popular suggestion among some of the people who gave evidence to us that if you are a local authority and you want to access communications data you should get a warrant. I notice from your evidence that you are not at all convinced about this.

Sir Paul Kennedy: No.

Baroness Cohen of Pimlico: Would you like to tell us why you think the SPOC process beats a warrant?

Sir Paul Kennedy: One can tackle this question from the other end in a sense. I do not see any justification for making local authorities get a warrant if you are not going to make a police force get a warrant. You are dealing with the same type of material from the same source, and volume considerations, apart from anything else, suggest that that would be wholly unworkable if we introduced it in relation to 500,000

applications for information. If the system can be properly worked, as it is by some local authorities, for example, it provides a very high degree of safeguard. The applicant in the housing department, or wherever, or market traders or something like that, has to make an application that goes to be considered by a senior member of staff not involved in that particular investigation, and he or she then gives the authority for it to go to the next stage.

The problem—and I have hinted at this already this afternoon—is that a number of local authorities do not use their powers very much, perhaps because they are not very big authorities or they do not have particular types of problems. When they come to use them they do not necessarily get the procedure right, and that causes problems. Happily, there is a thing called NAFN, the national association—you have probably heard about NAFN, and I have mentioned it. NAFN has established a central authority that they can use, and it is hugely efficient. We have inspected both of its sites more than once and it gets it right. Some 70% of local authorities now use NAFN and the number is rising. Should the others use it? For the most part, yes, but I am not going so far as to say that I think you should necessarily make it a statutory requirement to use it. What I would quite like is for it to be made easier to use. The ones who do not use it do so on financial grounds. They say, “It would cost us something to use NAFN”. If a formula could be devised that would take away that hurdle, I think that then the probability is they would use it too and the question would almost disappear, because there would be a satisfactory way of local authorities processing their applications, which would be every bit as good as MI5.

Baroness Cohen of Pimlico: I suppose the civil liberties argument is that you do not give powers to them that you do not feel that they really need.

Sir Paul Kennedy: Yes.

Baroness Cohen of Pimlico: You are perfectly comfortable in giving the police and security services powers, but you are saying that the procedures are in fact exercised in the same way.

Sir Paul Kennedy: Yes, the controls are perfectly in place. I know there has been the odd incident about the school catchment area, or something like that, but they are the odd incident and if there is a criticism—and I have said this in a report before—it is that local authorities do not always use these powers as much as they perhaps ought to, to deal with the type of offending that they are entitled and required to investigate, and probably have no other means of investigating.

Q679 The Chairman: When you say "local authorities", you do not just mean local councils; you mean they are the public authorities.

Sir Paul Kennedy: Yes.

The Chairman: So, HMRC, the Fire Service, the Department of Health—those people.

Sir Paul Kennedy: HMRC is quite a big operator, so it comes on the other side of the fence. Some of the others, as you, Lord Chairman, said, like the fire service, are exactly on this side of the fence.

The Chairman: So the encouragement you wish to give to those others to move on to what in the Committee we nickname the "super SPOC system", you would extend that out as far as—well, let us keep the security service out of it—the police, who are doing their own SPOC thing, HMRC possibly, but everyone else you would like to see covered by the super SPOC.

Sir Paul Kennedy: If you take out the intelligence services and the police, and HMRC—SOCA I envisage being part of the police—I would be perfectly happy with everyone else using NAFN. The problem of course is that an awful lot of them are not

local authorities and NAFN is a local authority body, so something would have to be done. I do not think that is impossible to enable the Mersey Docks and Harbour Board, or someone like that, to be able to use a body that is not theirs.

The Chairman: You think that would give a higher level of certainty, safety and accuracy than trying to use their own internal SPOC systems, or even a magistrate's warrant.

Sir Paul Kennedy: Absolutely, yes. That would certainly be so other than with perhaps the very large authorities. The City of Birmingham, for example, as a large authority may have enough traffic to develop quite a degree of sophistication of its own.

The Chairman: What about the FSA?

Sir Paul Kennedy: The FSA has quite a lot, too. It is one of the biggest users.

The Chairman: Thank you, I found that very helpful.

Q680 Dr Huppert: Sir Paul, your submission suggests that you want to keep the number of permitted purposes that communications data can use. You will be aware it is a long list, from national security to any crime and to collecting any tax or duty, and so forth. Is that right that you want to keep all of that full list?

Sir Paul Kennedy: Yes. I do not see any reason for not keeping it. I am not wedded to this, but I think the reality is some of these are quite important even though they have not cropped up recently, if one can put it that way, yes.

Dr Huppert: You are presumably aware that Mick Creedon, who is the Chief Constable of Derbyshire Police and the ACPO lead on serious organised crime, commented—and I believe it is a direct quote—"If I am driving on the motorway and I see someone on a phone texting at 80 miles an hour, that for me would pass the test

immediately". He is technically right that it is a crime. Would you agree that that was a proportionate use of communications data?

Sir Paul Kennedy: I have hesitations about it. I agree. I read that, like you. But on the other hand I am doubtful about the serious crime frontier, if we are in that territory. It arises more particularly and more frequently in relation to local authorities. They have a statutory duty to investigate fly-tipping. It is easy when it does not affect you or me to say, "Not very important crime", but if it affects you directly it is very important to you, and the only way in may be to find out who owns the mobile number on the card that was given to the householder.

Q681 Dr Huppert: Can I go back to your role of inspecting this? Let us say Mr Creedon authorised the use of communications data for somebody who was texting at 80 miles an hour. You then inspected that. Would you say, "This is perfectly legitimate, it is a crime. It is fine"? Would you raise questions about it? Would it fall into your category? Would it push the Derbyshire authority down towards "satisfactory" or "poor"? Would it have any effect at all?

Sir Paul Kennedy: It must depend entirely on context. There was a case on the M1—I cannot remember the name of the person who was involved. A child was killed, and you will remember it too probably, near Sheffield. The suspicion was that the driver had been on his mobile phone at the time when the accident occurred. Now that is a pretty serious matter, is it not?

Dr Huppert: Sir Paul, the example that Mr Creedon gave was quite clear, "If I am driving on the motorway and I see someone on a phone texting at 80 miles an hour", there is no suggestion of anything else; it is just 80 miles an hour on a phone. He believes that would be proportionate. He would go ahead with it, presumably. What

would happen when you inspected that authority? How would you look at that case? Would you flag it up as a concern?

Sir Paul Kennedy: I am being whispered to, so, Joanna?

Joanna Cavan: I do not think an application just on the basis of that one sentence, if that was all there was, would even reach the SPOC, and get through the SPOC, and it would not even go to a designated person to consider. In the robust guardian and gatekeeper role that the SPOC performs, they will be looking for certain tests to be met, and they are very professional and they take it very seriously. So if there was a lot more to that case, if it was dangerous driving and something happened and there was a lot more information, it could be that the communications data was required to prove that offence, but something just on the basis of that one sentence with no more detail, that would not—

Dr Huppert: Ms Cavan, you are hoping that the SPOC would say to their Chief Constable, "I am sorry, you are wrong, we are not doing this. I know you are the lead nationally for the police on this but I am not going ahead with it". That may be the case. Let us say the SPOC did not feel comfortable enough to tell their Chief Constable that they were wrong and approved it, you would then inspect it and have a look. You would see this. What happens next?

Joanna Cavan: Then we would ask for any further information. Obviously an application form should stand on its own, so that should have contained everything it needed to to justify the tests. If we are not satisfied that there is enough information there we will ask to look at the case file. We will ask for the applicant, and the designated person who approved that request, to provide us with their thoughts and justifications, if there are any policy logs around the decisions that were made and the reasons why. So we will look at whether there is any more surrounding

information or evidence, but ultimately if there is not we will conclude that we do not deem that request was necessary or proportionate.

Dr Huppert: I think that is very helpful given this disagreement there. So you would give him a chance to add to the information that was originally provided and to look back six months ago and say, “Actually, I think there was some other thing. I was very concerned about something else”? They would have that chance above what they asked authorisation for.

Joanna Cavan: Yes. I think it is really important because the quality of applications does vary and sometimes someone may not have put everything they needed into the application. Technically, that should not have gone all the way through if it is not of particularly good quality.

Dr Huppert: Would you flag it up that it was not of good quality, and that would again move people down the rankings?

Joanna Cavan: Yes. There are two areas. We will either conclude that the request was not justified or we will conclude that, on the basis of the information we have seen, the request was justified but it was not sufficiently outlined in the application on the case.

Q682 The Chairman: So you are making some judgment on proportionality. Would you like, Sir Paul, to see additional powers given to you on proportionality to make wider judgments?

Sir Paul Kennedy: I do not think so. The situation is entirely as has just been described to you. I think that in judging or reviewing other people’s judgment one has to keep that in mind also, that you are deciding whether or not the application was justified. You are not the first-instance decider. That is quite an important distinction to keep in mind. What has just been said, of course, is entirely true—that if the

paperwork is not up to standard you certainly see what the paperwork was founded on. When you then look at what it was founded on you may be able to say, “Well, even though it was not up to standard it was clearly a necessary and proportionate act to exercise the statutory powers”.

Q683 Mr Brown: Our constituents worry that information about them that ought to be confidential will be discovered and then improperly disclosed, and this could be everything from a public official with access finding out something about somebody they know, to public officials obtaining information on, say, a celebrity or a person in the public eye and selling it to the newspapers. We know these things happen. If people do such things, should they not be caught and punished?

Sir Paul Kennedy: Yes, it is a criminal offence to misuse the powers.

Mr Brown: I think the offence is misconduct in public office.

Sir Paul Kennedy: Yes. No difficulty about that proposition. I do not—

Mr Brown: How many such prosecutions are there?

Sir Paul Kennedy: Of misuse within our sphere?

Mr Brown: Yes.

Sir Paul Kennedy: As far as I know none. But if people are wanting to acquire information of that kind they do not use legal means, not normally.

Mr Brown: I understand that, but what the public are looking for is safeguards against that, and catching people and punishing them would be one safeguard.

Sir Paul Kennedy: As far as I am aware, there is no misuse of that kind within the area in which I operate. That there is misuse of that kind I know as well as you because I read my newspapers.

Mr Brown: I think the public’s fear is not so much in the area in which you operate but—

Sir Paul Kennedy: Legal intercept does not give rise to that type of conduct.

Mr Brown: No, but the information is being shared with others and then comes into the public domain. The route is not a direct one; it could be an indirect one.

Sir Paul Kennedy: I cannot immediately bring to mind any recent instance of information being leaked, which has been obtained for a proper purpose, if that is what you mean.

Mr Brown: If we were looking for a way to reassure our fellow citizens that the citizen was safeguarded against such an abuse, how should we go about it?

Sir Paul Kennedy: I have absolutely no doubt that, if that happened, there would be appropriate measures taken, probably in the form of a prosecution, yes.

Mr Brown: Do you think the courts would be supportive?

Sir Paul Kennedy: Yes. I do not think there is any difficulty. If you obtain information in the course of your duties under RIPA, and you disclose it to someone else, you are committing a criminal offence if you disclose it to somebody who should not have it. It is a matter of concern to people such as, for example, the IPCC, yes.

Mr Brown: Our fellow citizens are not reassured. That is just a common line.

Sir Paul Kennedy: The powers are there and they would be exercised.

Q684 Lord Strasburger: Sir Paul, on pages 42 and 43 of your report, you have identified two local authorities where 52 requests were not in accordance with the law. I would like to know, if you know, what penalties or sanctions were applied to the individuals or the authorities in those cases.

Sir Paul Kennedy: Sorry, what page?

Lord Strasburger: Page 42—the bottom of 42 and the top of 43, 52 requests not in accordance with the law. What happened to those individuals and those authorities?

Joanna Cavan: In those cases they obviously received poor compliance in those areas and the recommendations would be that, if they are going to take those cases to court, they should inform the prosecutor that that data has not been acquired in accordance with the law, and then that will be up to—

Lord Strasburger: But what happened to the people who failed to comply on a large scale?

Sir Paul Kennedy: We report to the person who is in charge of them. What happens to them on the ground is a matter then for those individuals. I do not have a remit to prosecute.

Joanna Cavan: I think it is important to distinguish as well whether it was wilful or reckless use. In these cases we were satisfied that they did not intentionally breach the legislation, it was just lack of knowledge and lack of training that led to these unfortunate errors, but it will be up to the local authority to decide. In one of those local authorities they ceased to acquire communications data until they were satisfied they had put robust systems in place to prevent recurrence of similar errors.

Q685 Mr Brown: Should you have a remit to prosecute?

Sir Paul Kennedy: In some respects I am half inclined to say yes, but on the whole I would prefer to say no, because the way in which we operate, for most of the time, is to try and encourage compliance and not to act as some kind of dragon who is there to try and notch up how many errors you have made. Yes, we want to count errors but we want to try and ensure that local authorities do it right. That is why, for example, we have been hugely supportive of NAFN because we know NAFN does it right. What we are more inclined to say is, “You got it wholly wrong, please use NAFN”. I think that is a more effective way, from the public point of view, of getting compliance than saying, “We will prosecute you”.

Mr Brown: If you uncovered something that you felt ought to be prosecuted, who would you ask to prosecute it?

Sir Paul Kennedy: It depends on the context. If it was within a police force we would probably go, in the first place, to the Chief Constable and say, “Here is the matter. What are you going to do about it?” In the last resort I can of course go to the Director of Public Prosecutions and say, “There it is”, but we have not had to do that so far.

Mr Brown: Thank you very much.

Q686 Dr Huppert: Sir Paul, your written evidence says, “It would be helpful if the record keeping requirements were extended to collect statistics in relation to the number of applications, the necessity purpose under which the data was acquired and the specific offence or crime under investigation. This would enable more meaningful conclusions to be drawn and would provide a further indication as to whether public authorities are using their powers appropriately.” If organisations are not keeping the statistics about application numbers, the purpose and the offence or crime, how do you verify that they are behaving proportionately?

Sir Paul Kennedy: The answer is they do keep the statistics but if they were required to keep them it would be much more accessible.

Dr Huppert: So they keep them in an inaccessible way. What are you saying? They either collect them or they do not, surely.

Sir Paul Kennedy: They all keep them differently, or not a lot of them keep them differently, and what we are trying to do is to say it would be a great help to us if they were required to keep them in a way that would be easily accessible so that we can present figures to you of applications. At present we cannot do so without getting co-operation from a whole lot of different people.

Dr Huppert: Your written evidence says that you want the requirements to be extended to collect statistics.

Sir Paul Kennedy: Yes.

Dr Huppert: Which is not quite the same as saying, "I want them in a format we can read". Which one do you—

Sir Paul Kennedy: Both. We want them in a form that can be read too, yes.

Joanna Cavan: At the moment they would need to trawl their systems and there would be an element of manual counting, which obviously is not feasible when you are talking about thousands of requests. So, yes, they can find the information out for us and quite often we do put more specific requests when we go to inspect around certain types of data, certain date periods, certain statutory purposes, but depending on what system they are working on it can be quite time-consuming for them to do that, because the systems have been built around the requirements in the current code of practice. So if the requirements are updated and there is a new list of information that they must provide statistics for on an annual basis, then the systems will be able to be rewritten.

Dr Huppert: What you are saying is that we could have a system where of the 500,000 or so requests a year it would be possible for, say, this Committee to be told how many there were for which crime, how many for what sort of purpose and so forth, which we simply cannot do at the moment?

Joanna Cavan: Yes.

Q687 The Chairman: Would you be happy then with a schedule attached to the Bill setting out a standard format for reporting or something like that?

Joanna Cavan: I think it would normally be introduced through the code of practice.

Sir Paul Kennedy: In the Bill there would have to be a code of practice, so the opportunity is there for this particular suggestion.

The Chairman: It seems ironic we have a Bill that allows the automatic interception and collection of billions of bits of information but there is no method by which you can automatically get the information to publish.

Sir Paul Kennedy: I agree.

The Chairman: It would seem to me that what is sauce for the goose and so on.

Q688 Stephen Mosley: Some of the witnesses we have heard have suggested that individuals should be notified if their communications data had been obtained by an investigator under the RIPA powers—I guess there is an exception there if there is a criminal case that is ongoing or something—but do you have any views on that?

Sir Paul Kennedy: I do not favour it. Almost all the mistakes lead, for example, to your mobile telephone number being obtained and nothing happens, but an error has been made. For you then to be contacted to be told that your mobile telephone number was obtained by error does not seem to me to take anybody anywhere further forward. The vast majority—and I am speculating now, I agree—of these inquiries arise out of a criminal investigation in some form or another.

It is also worth remembering, as one goes along, that we see—not a lot—from time to time investigations that have resulted in innocence being proved. What do you do about those? Somebody may have come into the frame and then the data investigation has shown they are not in the frame. I do not think they should have to be told that they were ever in the frame. If you look at what comes out of an error you very soon find that it is an error simply because nothing has come out of it and I do not think the individual would learn much by knowing, “I was the subject of an error”.

Q689 The Chairman: Sir Paul, I thank you very much for your patience—we are running a little bit late—but finally could I ask you about the filter? You said you may be slightly vague about what the filter will be at the moment but we have received evidence questioning whether the results of the filter will meet evidential standards given that no one entity could be in a position to say, "That is my data from Mr X going to Mr Y that travelled down our line only". If we have deep packet inspection, which is picking up bits and pieces with regard to a BT line, a Vodafone line and a Facebook channel, they might not be able to say to the court, "We can vouch for the call sanctity of this package". Have you a view on that? Are you aware of it?

Sir Paul Kennedy: Not a complete one because I think it would have to be tested in reality at the end of the day. But it is not unfamiliar to have evidence that comes from a source that is restricted. One can think of other examples of that where Parliament only permits you to do a certain thing, and that is what you obtain as a result. The fact that this falls in that category does not, of itself, mean that it will not be acceptable as evidence. It will come from a controlled source.

The Chairman: If I could clarify, I think what our witnesses were suggesting was that defence lawyers would be easily able to drive a coach and horses through it because hypothetically BT would say, "Well, here is what we have encrypted but we do not know if that is the Facebook bit or the Yahoo bit or someone else's bit and we cannot vouch that that is accurate".

Sir Paul Kennedy: I do not think that at this stage it is possible to give a firm answer to that, but it is not necessarily a no at all. Furthermore, in this field an awful lot of the information you are seeking is an order to forward an investigation. It may in the end never require to be used in evidence—and that is certainly true, for example, about the argument in relation to interceptors' evidence. We get a lot of information that is

very valuable and it is never used in evidence, so I do not think that that aspect of it is anything to be terribly worried about. We can deal with it when the time comes.

The Chairman: Mr Huppert on this point, because we are running rather late.

Q690 Dr Huppert: Presumably, as communications have become more complex, more and more of the data would be received through the filter, so if there are questions about the evidential nature it would mean that effectively you would be less and less likely to be able to use any of this communications data in a court.

Sir Paul Kennedy: It would have to be tested. I am just not prepared to say that it is inadmissible. I think it might be admissible.

The Chairman: Sir Paul and Joanna, thank you both very much. I am sorry we started late. We have overrun. That is testimony to the quality of the evidence you have given and the interest colleagues have in it. Thank you very much for coming. I wish you a happy retirement as from 31 December this year. Thank you very much.

Sir Paul Kennedy: Thank you very much. Thank you for listening so carefully and receiving us so courteously. I hope we have been of some help. If there is anything more we can contribute, we are very happy to do so.

The Chairman: Thank you very much. We will go straight on to our next witness and keep our fingers crossed for a vote, or keep our fingers crossed for no vote.

Examination of Witness

Christopher Graham, Information Commissioner

Q691 The Chairman: Mr Graham, thank you so much for coming, and profuse apologies that we are 30 minutes late. We were starting 15 minutes late because of a vote and we even then overran talking to Sir Paul. Thank you very much for coming. Just for the record, could you state who you are?

Christopher Graham: I am Christopher Graham. I am the Information Commissioner. I have been the Information Commissioner since June 2009. The Information Commissioner's role is to uphold information rights in the public interest, promoting openness by public bodies and data privacy for citizens. I have responsibility for enforcing the Freedom of Information Act and the environmental information regulations. For these purposes, the Data Protection Act and the privacy and electronic communications regulations are relevant.

The Chairman: Thank you very much. We are very grateful for your written evidence. You have nothing to add to that by way of introductory statement, I take it.

Christopher Graham: No.

Q692 Lord Faulks: Thank you very much indeed for your detailed written submission, Mr Graham, which we have all read. You make the point that it is for the Government to make their case effectively for this Bill but that some people might find their proposals difficult to justify, requiring the obligations that they do on providers. What category do you fall into?

Christopher Graham: You have quoted the second part of the statement. All I was seeking to point out was that there is a judgment to be made between the security community who say that we have to have this stuff and the civil liberties community,

which says that this is a gross invasion of privacy and citizens' rights. It is a judgment. To say that it is a judgment does not mean you have taken the judgment. That is for Parliament and for this Committee, having heard all the evidence.

For the Information Commissioner, the interesting questions are the practical ones: how this regime might work if Parliament decided it wanted to go ahead with the project. All I would say on the principle of the thing is to recall that six years ago my predecessor, Richard Thomas, sounded a warning that we were in danger of sleepwalking into a surveillance society. I think that had the very salutary effect of waking us all up. I do not think anyone would say that we are now sleepwalking. The evidence that you have already had, both written and in person, shows very strong arguments either way. The decision is for you and for your parliamentary colleagues to take.

Q693 Lord Faulks: Does that answer you have just given tie up very much with your very helpful recommendations about post-legislative scrutiny and the need for it to see how these possibly extended powers are progressing and possibly even to build in sunset clauses to the Bill?

Christopher Graham: That was a very strong recommendation that we made to the House of Commons Home Affairs Committee, which takes an interest in this sort of thing. We commissioned a report on the state of surveillance in the UK, and we pointed out that it is all very well for Parliament, with the best of intentions to pass legislation. The thing is to see how it has worked in practice. That is what is happening with the Freedom of Information Act at the moment; the Justice Committee in the Commons has been conducting post-legislative scrutiny. This is jumping a few fences, is it not? It would be a good idea, if this Bill went forward, I will not say that a sunset clause be written in but certainly for a review to be envisaged,

because on the face of it is a question of assessing the risks, and there are important data protection principles at stake. Whether the processing is fair and lawful is the first principle. The issues are very often around the seventh principle of security. There is a fifth principle about the retention of material for longer than is perhaps required. There is the principle of good practice of data minimisation. I think everyone would be concerned about the possible unauthorised access for retained material and perhaps the unlawful exploitation of the retained material, so it is really is for Parliament to keep a watch on these things. You can have commissioners charged with doing this and doing that, but this would not be one to legislate on and forget, I would suggest.

Q694 Baroness Cohen of Pimlico: What strikes me about this is that you have been given the duty, but I am not quite sure how you are going to do it. The only powers you are given under the draft Bill are those in Clause 22(5). Are these going to be adequate to enable you to protect the public? Is that what you think you are going to be required to do?

Christopher Graham: I am intrigued because, as you say, it is a duty but I do not see the powers. I have not heard from the Home Office whether this is merely an expression of the responsibilities that the Information Commissioner has anyway in relation to data protection or whether something new and extra is envisaged, because if one is going to be part of a framework of reassurance where safeguards are built into the Bill, frankly it has to be more than aspiration. I am told that I am to keep things under review, but I would like to know how and with what. I imagine that there would need to be some sort of inspection regime of the kind that Sir Paul has just been describing. I would like to think that if the safeguard was found to be

credible, it would involve powers of audit of the communication service providers who have been designated under the Act, whoever they are.

I have to tell this Committee that I do not have those powers of non-consensual audit. I am asking for them in relation to local government and the health service, but I am not getting very far. I have those powers in relation to the privacy and electronic communications regulations for some communication service providers but only in relation to those regulations, so if the Home Office means that the Information Commissioner is really going to be able to reassure citizens that these communication service providers, whoever they are, are hanging on to the information satisfactorily and are getting rid of it finally and irreversibly after 12 months, I need the powers and the resources to do that, and if all there is is Clause 22 of Part 3 of the Bill, I am sorry but that does not do it.

Baroness Cohen of Pimlico: Thank you very much. I did not think it did either, so I shall be interested. We will have to ask the Home Office what they thought they meant. I loved Annexe A of your written evidence because the surveillance road map is just incredible. It is staggering as to who looks after what and who appeals to what. Do we see a need for a wholesale re-approach to all this, because it looks to me as though they have just handed you a few other clauses that put on you a duty to look after something else still but you do have nothing to do it with. It is difficult if you ask who is responsible for the freedom of the citizen. If the answer is that you are, I am not sure you quite have the powers anywhere.

Christopher Graham: The road map was designed with the co-operation of my commissioner colleagues in different parts of the wood to explain how the terrain runs. As I say in the copy that you have had, it is very much a work in progress because things are moving all the time. For example, Mr Andrew Rennison has been

confirmed as the Closed Circuit TV Commissioner, so there are some things to add there. The powers that be are in the process of appointing a Biometrics Commissioner, and so on and so on. It is a living document and was designed partly to make sure that there was very good communication between our various officers and that our staff understood how we should be working closely together. Also, now that it is in the public domain—and I do not think that a document like this has been designed before to inform the citizen of who can help—it identifies where there are gaps and where there are overlaps. It shows that some of us have powers to deal with complaints and others do not.

The Home Affairs Committee in the Commons that recently considered these things concluded that there ought to be either a single privacy commissioner or a sort of primus inter pares, and we would all be organised into one office. It sounds superficially attractive until you come to the Information Commissioner and you realise that my responsibility is both about privacy and about open government. I need to be able to take delicate judgments about when the data protection side needs to be paramount and when the freedom of information side needs to be paramount, so you could exclude me from some sort of single system. You do not need to have a single system and everyone in the same premises if we all understand what our various roles are. That was the aim behind the road map.

Q695 Dr Huppert: I will start with issues about how you keep security under review. One of the issues that many of us are concerned about is that data that is being kept may be inadvertently lost. Your office put out a statement today about a rather significant loss from Greater Manchester Police: the theft of a memory stick containing sensitive personal data that was not protected in any way and had the details of more than 1,000 people with links to serious crime investigations. I think

you penalised them with a penalty of £150,000. Is this an issue to be concerned about with other collections of data?

Christopher Graham: That is the 26th civil monetary penalty we have had to impose. Greater Manchester Police got away with £120,000 because they got a 20% discount for early payment. We are a very reasonable authority. Nevertheless, it is undoubtedly true that the public service is not as good as it should be about keeping information secure. We have to work on that, which is one reason why I have asked for the power of audit, first of all of local government, which is particularly bad, and then of the health service, where the information is obviously very sensitive. Greater Manchester Police is not the first force we have had to issue a civil monetary penalty against. I remember the Lancashire constabulary quite recently had information about a very vulnerable missing teenager simply blowing down the street because the file was left in a squad car.

This is a worry, and it is a worry that the penalty for unlawful disclosure of information is so unconvincing. It is a fine-only regime, at the magistrates' court at least. Section 55 of the Data Protection Act is not a very scary provision. There is work to do for Parliament, and I hope very much one of your conclusions may be to support the conclusions of the Home Affairs Committee in the Commons or the Justice Committee in the Commons that we ought to get on and commence Sections 77 and 78 of the Criminal Justice and Immigration Act 2008, which have the potential for a stiffer penalty to be imposed. I am not sure that is going to get us very far in relation to what you are dealing with, because Sir Paul made the distinction between context and content, and communications here are supposed to be about context. So, yes, if my staff and I were asked to take on this role we would carry out our duties

conscientiously, provided that we are given the resources—we would do it anyway, but we need the resources to do it, which is another story.

It is not quite the same thing as losing an unencrypted memory stick with the details of rather a lot of police informers.

Q696 Dr Huppert: Thank you, that is quite helpful on some of the security issues. You highlighted a number of concerns; I will come on to another one in a second. I ask this particularly because I note that the Conservative policy coming into the last election said, "Immediately submitting the Home Office's plans for retention of and access to communications data to the Information Commissioner for pre-legislative scrutiny". Did you have that opportunity?

Christopher Graham: When I came in, in 2009, this was a very live issue. I remember having a very fierce letter from the then Home Secretary before I had even been appointed saying that the interception modernisation programme, as I think it was then called, was an absolutely priority and that I must realise that we live in a world of terrorism and serious crime and must shape up generally. I said, "How very interesting, I look forward to discussing it with your officials". The only discussions I have had with Home Office officials over three years have been about the theory. I have had a series of presentations where I have been shown a model of how communications capability is degrading, and the 75% figure is very familiar to me.

My staff have then, because we were fairly sceptical in the evidence we put in in 2009 to the previous Government's proposals, worked with the Home Office on doing a proper privacy impact assessment and the privacy impact assessment, which I think was published at the same time of the Bill. We certainly followed an ICO model of how these things should be done. At the end of the day, it comes down to that judgment, which is where you come in.

What I have not had is any discussions with the Home Office about how the regime is expected to work. I did not see the Bill. I saw the draft clauses that concern the Information Commissioner I think the day before, possibly the week before. I have had one telephone call with the Minister responsible since, and that is it.

We really do need now to get into the nitty-gritty of how this regime would work. It was very interesting that, of the 449 pages of evidence that were submitted to you in the first wave—I have not gone through the latest lot—there was only one estimate of the scale of the information that would be retained. Someone said that if you take 1% of all the internet material in the UK over a year, you get to 10 petabytes. I did not quite know what a petabyte was but technologists here will recognise that it is one hell of a lot of material. It is actually the same amount that Facebook identified in a prospectus for its recent initial public offering of all the audio and all the video that it retains. So we are talking about a billion customers worldwide of the most successful social network. That is the scale of what we are dealing with.

If I am going to be asked to keep that under review to any purpose that a citizen would find reassuring, that is some task. I do not quite know how I would set about doing it because I do not quite know, and I do not know whether I am going to be told, who the communication service providers are. Even when I know, I will need to have the resources to do the annual inspection that I suppose would be required, but then I also need to recruit the technologists to undertake the sort of spot checks that your constituents and citizens would find convincing. So I would need the powers and the resources to do that, and we would need to get into very detailed discussions with the Home Office to find out how it envisaged that this would work if the Bill proceeded.

Q697 Dr Huppert: I will very quickly pick up on one thing that you mentioned and that I was going to raise anyway: the list of service providers who are required to keep this data. According to your written evidence, the Home Office will not tell you on the grounds of national security who you are supposed to be checking up on. Is that right and is there any promise that it would change that in the new regime?

Christopher Graham: I only know what I know. You might say, "Well, you have not asked", but I am sort of waiting to see how this process continues. It is not rocket science. The six largest ISPs in the UK account for 95% of the traffic, so I assume that British Telecom, Virgin Media, TalkTalk, Sky, O_2 and Orange will be candidates.

Dr Huppert: You would not know whether a small provider was or was not, and hence you would not be able to check whether or not they were complying.

Christopher Graham: If nobody tells me, I will not check, so that is no great reassurance. Also, I hope that I am not being overly sceptical, but I notice that the ambition is to increase the capability from the existing 75% to 85%, which leaves 15% still uncovered. Again, I do not think I am saying anything that is wildly controversial when I point out that if you are the international terrorist or the organised criminal who this system is designed for, you will presumably have the wit not to go with one of the big six. You will find a small provider, and you might even be able to afford the £5 a month to buy a virtual private network registered overseas. All your traffic will then be encrypted and you are home free.

I think the really scary people will have worked that out for themselves, so basically this is a system that, on the face of it, is looking for the incompetent criminal and the accidental anarchist.

Q698 Michael Ellis: Could I just make an observation, Mr Graham? If I may I will characterise what you seem to be saying at the moment as something of a power

grab on your part, because you have made several complaints, it seems to me, that your powers are insufficient to do certain things. You want to increase the penalty powers, you want to increase your audit powers, you do not want to share powers with other commissioners as you do not think that would be right, your authority would not work as far as working with other commissioners is concerned, but it is the taxpayer who is penalised when police services are fined vast sums for losing memory sticks. Is it a fair characterisation that you are looking for more power from the Home Office and from Government?

Christopher Graham: I am looking for more powers to do the job that Parliament has given me to do. I merely make an observation about the safeguards and the limitations, which we called for when we put in our response to the 2009 consultation on the previous scheme. Apparently part of the reassurance is the Information Commissioner will be asked to keep something under review. All I am saying is that you want us to keep it under review. It is not a power grab to say, "I will need to have the resources to do it". Sir Paul just now said he had been assured that what 'we need we will have'. I have received no such reassurance. The only resources I have on the data protection side are the £35 that data controllers pay for the Information Commissioner's Office. The scale of the task is absolutely massive. I do not think it is a power grab to say, "Give us the tools and we will begin the job".

Michael Ellis: The Interception of Communications Commissioner has received an assurance.

The Chairman: There is a Division in the Lords. We will need to suspend for a few minutes and we will reconvene as soon as enough Lords are back to make us quorate. Officially it is 15 minutes but we will try to be faster than that. Thank you.

The Committee suspended for 8 minutes for a Division in the House.

Q699 Lord Faulks: Further to the last question, I can probably anticipate your answer: you have obligations to keep a lot of things under review as a result of this draft Bill. The evidence we have so far had suggested the notices issued under Clause 1 will not be published. Have you received any assurance that notices will be available to you?

Christopher Graham: No, I have not. As I said, the work that will be necessary with the Home Office has not taken place yet. That is no criticism of the Home Office. I am sure that when you talk to Home Office witnesses at the end of this process, you may get more information than I have had up to now. I merely make the very simple point that if I do not know who has been the subject of an order, I am not going to be able to keep them under review.

As a postscript to Mr Ellis's question before we were interrupted by the Lords' Division Bell, I should just make clear that although the civil monetary penalties that I have the power to levy in respect of serious breaches of the data protection principle are up to £500,000, that money does not stay with the Information Commissioner but goes to the Consolidated Fund. So I do have this resources problem, not like my Spanish colleague, who raises the money for his office by fining people. Nor should it be like that. Just because £150,000—or £120,000, as it turned out—has been taken from the Greater Manchester Police, that does not help me any.

Q700 David Wright: You are also required to keep under review, Mr Graham, the destruction of data. I have read your submission notes. It is clearly important for the public to know that data is being destroyed appropriately. What is your reading of the content of the Bill, and how are you going to potentially achieve that review? Having

read your evidence, I envisaged groups of people potentially sitting in yards outside office buildings putting sledgehammers through material in order to physically destroy data that is held. What is your view on this?

Christopher Graham: Again, it is more likely to be the very effective overwriting of information that is held wherever it is held. The first thing I would have to do would be to employ specialist staff to complete this work, given the complex and technical nature of what is being asked of us. I will certainly need the compulsory audit powers under the Data Protection Act to be able to take on that work. These are all conversations that we need to have, but obviously the public will need reassurance that the obligation to delete will be honoured and there will not be a temptation on the part of communications service providers having been asked to hang on to material that they would not have hung on to in any other circumstances to do something with it. That clearly is quite unacceptable, and we have to have a credible regime that can stop that happening.

David Wright: Other witnesses also have doubts about the practicality of destroying evidence so that it can never be retrieved, and one suggested that it would be more appropriate to repeat the requirement of the Data Retention (EC Directive) Regulations 2009, which is to, “Delete the data in such a way as to make access to the data impossible”. Reflecting what is possible today, would that be an improvement to the draft Bill?

Christopher Graham: I am not sure that it makes a great difference to mess around with the definition. You might just create problems in another part of the wood. The vital thing for this Committee to satisfy itself about, when you have heard from the Home Office, is how you can be sure that whoever is asked to carry out this

inspection, whether it is the Information Commissioner or one of the other arrays of commissioners, is able to do the job in practice rather than just in theory.

David Wright: But your submission to us did say it is not clear how the requirement to destroy data relates to the way in which operators achieve the deletion of existing records in practice. Basically what you are saying is that the Bill as currently drafted does not clearly indicate what “destroy data” is. You have given us a comment today that you think it is potentially the overwriting of material. Would it not be better if this Bill specified exactly what “destroy” meant?

Christopher Graham: It is possible. My major concern is to understand how the supervision task—this is my perspective—is to be carried out with any credibility.

Q701 Baroness Cohen of Pimlico: What you are telling us is that you have not had the conversations with the Home Office on how you are to do all this, which you would expect to have and indeed that you have to have. Is it a fair question to ask whether you have made any calculations inside your organisation on the extra resources and extra staff needed to enable you to do any of this? We are thinking with one part of our minds about the cost of doing all of this, and the Home Office has provided us with an estimate, but I am not sure that it was thinking about the Information Commissioner. I may be doing it an injustice, but I am not sure that they were.

Christopher Graham: I hope the Home Office does not think this is something that I can do just from my own resources. It is the downside of the Information Commissioner being quite a high profile role at the moment and lots of departments of state having ideas such as, “It would be a jolly good idea to get the Information Commissioner to do this, that and the other”. In some ways it is good to be popular. On the other hand I have, as the chief executive, to keep my feet on the ground and

say, “Excuse me, who is paying for all this?”, because I only have the resources that I have and we have the usual Gladstonian rules about not using freedom of information money on data protection or vice versa. I do not think I would be able to use either of those sources of revenue on this task, which is over and above the usual run of data protection work. I would be looking to the Home Office for grant in aid, and if it has not done its sums it better had. It simply cannot be a credible reassurance if it is not an activity by the Information Commissioner’s Office that is sufficiently well resourced, both with people and with funds, in order to do the job. It just does not deliver.

Baroness Cohen of Pimlico: Have you made any calculations of the kind of number of extra people you would need?

Christopher Graham: This is a chicken and an egg situation, because until I know the scale of what I am being asked to do I cannot do the sums. I simply flagged up to you in my written evidence, and again now, that here is an issue that we need to pursue. This is a draft Bill. If it proceeds, we need to have those conversations, but obviously organisations such as mine are planning all the time and it would be good to know.

Q702 Lord Strasburger: I have a quick question on destruction. When you are reviewing the destruction of data, how confident can you be that all copies of that data have been destroyed on the basis that there are multiple copies for back-up purposes and so on?

Christopher Graham: We have learnt from bitter experience in other cases that sometimes the things that we have been assured have been destroyed appear in caches here and there later on, so it is certainly a challenge. One certainly would be looking for a regime based on audit assurances and then some without-notice

inspection. Again, it would be helpful to know the amount of retained material and therefore the scale of the audit task that I have to undertake. At the moment, all we have is a proposition but no detail.

Q703 The Chairman: On destruction, it would seem that one gap which the Home Office is concerned about is the social media providers: the Facebooks, Yahoos, Googles of this world. If they decide to co-operate with the Home Office and create the systems to collect and store their 10 petabytes of information on their servers in California, how are you going to inspect Mr Google and Facebook and so on and make sure they have destroyed it?

Christopher Graham: In that they are not within the jurisdiction?

The Chairman: They will be storing information on British subjects in their servers in California.

Christopher Graham: Or wherever the information is stored. Google is quite a good example, because at the end of the recent Google street view affair we persuaded Google Inc to volunteer for a good practice audit by the ICO. It did not have to do it—well, practically it did because it was in so much trouble, but I could not make it do it. We certainly found with Google that we were dealing with a professional outfit. It understands the business that we are in and we are talking to grown-ups. My colleagues in the Irish Republic have the same sort of grown-up relationship with Facebook, so it can be done. No doubt the social network sites that receive these orders from the Home Office will behave appropriately.

The interesting thing is what happens about the 5% of traffic that is going through the small providers that nobody knows about it. These can develop very, very quickly. I saw a graph the other day of the impact of the Angry Birds game on iPhones. Suddenly something becomes very fashionable very quickly in the same way that

some things that were incredibly fashionable then just tank. But over a very short period an internet service provider can grow from nothing, and I suggest that your organised crime and your terrorist groups are going to be using those guys. How quickly are they going to be designated by the Home Office? How quickly can we find out what is going on there? It is a very challenging environment and a very challenging task that we are being asked to undertake.

Q704 Lord Strasburger: Can we turn to judicial approval for access? If and when local authorities have access to data retained under the Bill, this will be subject to judicial approval. Some of our witnesses have suggested that access to data by all public authorities, including your own, and the security and law enforcement services should be subject to judicial review. What is your view?

Christopher Graham: I have to declare an interest. As you have just pointed out the Information Commission's Office itself makes use of the communications data in order to enforce the privacy and electronic communications regulations and the Data Protection Act, for example. That is a very important part of the weaponry that we have at our disposal to deal with the scourge of spam texts, unsolicited emails, and worse: the unlawful access to private information from databases in breach of Section 55 of the Data Protection Act.

You may say this is rather self-serving. I would say that the purpose for which the Information Commissioner might require that is always going to be slap bang in the middle of enforcing the duties that Parliament has given us to deal with. It is not going to be controversial. Sir Paul's inspectors go round the ICO and check that we are compliant with the Regulation of Investigatory Powers Act. I think that is a system that works. I was quite struck by the point Sir Paul made to you when he talked about the effect that a warrant regime would have on speed of access and the sorting of

information that is needed to deal with unlawful activities. It is only an opinion, but I am not particularly persuaded by that.

Q705 Stephen Mosley: I was going to ask you the same question as I asked in the previous session. We have had suggestions that individuals should be notified if a request is made about them. Do you have any thoughts on that?

Christopher Graham: Again, I do not think it is something for the Information Commissioner to give a view on, but if you ask me I will give you a private view. I think the only circumstances in which communications data would be lawfully requested—and if it was not lawful it would be caught by the inspection regime—will be because there would be something to be investigated. If we are saying that individuals then have to be notified, that could obviously be a problem in the course of an investigation. If the Home Office says that this is about serious crime and terrorism, that would not be a good idea. If people had been eliminated from inquiries, what is the point in telling them that they were in the frame but they are not now? From a citizen's point of view, I would not go down that route.

Q706 Stephen Mosley: Under the Data Protection Act, individuals can make requests to companies to see the data that they hold about them. The Home Secretary is able under Clause 1 to specify what data those companies hold on an individual. If they put in a Data Protection Act request, they would be able to see that information, so surely within a very short period of time people put in requests under the Data Protection Act, find out what data is being held, and are quickly able to work out which communication service providers are holding the data and what data they are holding. Do you think that the secrecy about the data retention notices and Clause 1 will soon be circumvented by people putting in data protection requests?

Christopher Graham: Concerned consumers and citizens would shop elsewhere if this sort of thing concerned them. Yes, they do have the right of subject access under the Data Protection Act. I do not think it is rocket science to work out if you are a customer of British Telecom, Virgin Media, TalkTalk, Sky, O_2 or Orange that you are going to be on the list. You do not need to put in a subject access request to work that one out.

As I say, I trust that the Home Office is at least going to inform the Information Commissioner which of these communications service providers have been designated, or I cannot do the checking.

Stephen Mosley: You say there are a number of providers that are obvious, and there are, but you surely must be able to imagine a situation where interested parties put a request to every CSP they can think of, find out what data they are holding and therefore know which ones are affected by Clause 1?

Christopher Graham: I cannot fault the logic of your argument. One can imagine that the volume of subject access requests that communication service providers would face would be unsupportable, quite honestly, if that is how constituents wanted to play it. The Home Office will surely consider the wisdom, or the unwisdom, of keeping the information about designated authorities to itself because it may, as you point out, be information that is outed anyway.

Q707 Stephen Mosley: At the moment, though, Clause 1 does say that it is in effect secret. Because it can be circumvented in the manner that we have just described, do you think that the Home Office should just be up front and open about who it is putting Clause 1 requests into and what data to ask them to hold because it would be found out anyway?

Christopher Graham: That is one for the Home Office. I suppose it might say that the whole business of communications capability is a consideration of the behaviour of criminal and terrorist elements and that you do not want them to know too much, but I am not sure that what is apparently envisaged in that part of the Bill is doable.

Q708 Lord Strasburger: On the separation of data and content, some of our witnesses have commented on the difficulty or even the impossibility of separating communications data from content, particularly in an encrypted situation but not only an encrypted situation. What is your view?

Christopher Graham: To many people, communications data is content. It is very informative. You do not have to delve into the substance of a message to draw conclusions about the sort of communications that people have, which is why the authorities might be interested in it. But then one can understand why there are civil liberties issues and why critics of these proposals are saying, "I do not want the state, in effect, to have access to the communications I am having with my doctor, with that mental health helpline", or whatever it might be. I am not sure that you can make the contrast between content and context, even though it is reassuring to know that this is about establishing who was talking to whom, where and when rather than about the substance of what they were talking about.

Lord Strasburger: I think we understand that the data can in a lot of cases give a very good clue as to content or pseudo content, but this question is driving at how easy it is to separate that data from the true content of the communication, and encryption is a particular area of difficulty, but we have been told by other witnesses that there are also other areas of difficulty in separating the content and the data.

Christopher Graham: Yes. I do not claim to be a technologist. Encryption, which of course is something that, while wearing another hat, I very strongly advise would

frustrate the purpose of this Bill to track the communications from someone who is of interest to the police with somebody else. It is not difficult to see that encryption is a good idea for security reasons. If only that memory stick that the Greater Manchester Police detective had stolen from his house had been encrypted we would not have the problem that we have. So the Information Commissioner spends most of his time going around urging everyone to encrypt everything, and of course good businesses do that. Individuals can do it too for £5 a month so, surprise surprise, they will. That then frustrates the whole purpose of this Bill.

The Chairman: Slightly hypothetically—and I do not want to put you on the spot—could you therefore envisage circumstances in which, if you do not get the resources you feel you need, you do not have the access you feel you want, and you are not given the information about the CSPs that are on the Home Office list, the Information Commissioner is going to urge the British public, “Encrypt everything, it is the only way we can protect your privacy”? That is a slight exaggeration, but I am putting it that way for effect.

Christopher Graham: We pretty much do that anyway. We certainly do it with companies, and I would not do anything so incendiary as to say, “Encrypt everything so you can frustrate the Home Office”. All I am saying is that there is a lot of encryption going on, and there will be more encryption. It is a fact of life.

There is another aspect to this Bill. I hope that the Home Office could convince me otherwise, but there is something a bit Canute-like about this whole thing in that we are raging against the onward march of the modern world. The 75% figure arises because of the spread of communication through the internet. It is just a fact of life. You can get from 75% to 85% if, if, if—or can you? But the terrorists and criminals you are interested in will respond, the technology is there to respond, so, at the risk

of mixing my metaphors, it could be a bit of a chimera. There is an objective which the security services tell us is absolutely paramount and that we must have, but is it achievable?

Q709 Lord Faulks: You described some current abuses. The Bill envisages further data being retained. Do you have any comments about the possibility of abuses if this Bill becomes law?

Christopher Graham: I am very concerned anyway about the security of information in large databases, whether they are in the public sector or the private sector. I do not think that as a society we take this nearly seriously enough. The fact is that if you are taken to the magistrates' court for the unlawful disclosure of information under the Data Protection Act, or for dealing with rogue employees or people who simply see a way of making a fast buck and selling information—possibly to journalists but not normally to journalists, actually, usually to claims management companies—or even in pursuing private vendettas or family disputes, the response from the court is pitiful. The going rate is a fine of £120; it is a fine-only regime. It has to take into account your ability to pay, and at the moment the going rate is £120. If you are a private investigator and you are in the information business it is just a business expense and you go on your merry way.

I have spent three years urging parliamentary committees to commence Sections 77 and 78 of the Criminal Justice and Immigration Act because it contains the power to impose a penalty up to and including prison in serious offences. Of course what it does is to access all those potential deterrent penalties, community penalties, and so on, which the magistrates' court simply cannot do at the moment because all you can do is say, "We are going to fine you and, oh dear, you do not have any money, so it is £120". We have to take this more seriously, particularly if we want to get all the

benefits that the internet and online can offer for the effective and efficient delivery of public services. We have to get the confidence of citizens behind sharing data, for example, provided that is done sensibly and legally. You will not get that confidence if all people read about in the newspapers is that this local authority lost that piece of information, or this police force lost that piece of information. We will not get the confidence unless we have an effective deterrent regime in place, and we do not have that now.

Lord Faulks: You have given evidence along these lines in the context of the Leveson inquiry, have you not?

Christopher Graham: I have. I have to say that one of the despairing things about my otherwise fascinating job is that I have been saying the same thing for over three years and I am beginning to think it must be me, because parliamentary committees have bought the argument and reported and absolutely nothing happened. I hope I have convinced Lord Justice Leveson, but we will have to see.

Lord Faulks: You specifically refer to the police forces routinely accessing individuals' mobile phones on arrest. They gain access to information held on the phone even though the people may not be suspected of any wrongdoing. Do you understand that to be a lawful use of that opportunity?

Christopher Graham: My office is currently investigating the lawfulness of these cases that have come our way and what steps can be taken to prevent it. When we have reached a conclusion I would be very happy to update the Committee, but there seems to be a distinction between a policeman on arrest looking to see who is on your mobile phone, who your associates are, who you text, and looking at the content of your messages, your inbox, the names and so on. I am concerned about this but I

do not know what the answer is. As soon as we have a conclusion, I would be very happy to update the Committee.

Q710 Mr Brown: Can you tell us something about the mutual legal assistance process? For example, do you have any direct supervisory role over it, and do you think it is effective?

Christopher Graham: We do not oversee applications for mutual legal assistance involving communications data. We have no involvement on compliance issues on which to base any view about the current process, and I understand that the UK-relevant central authority is the Home Office, so I cannot help you, I am afraid.

Mr Brown: But should it be you or is it best that it be left with the Home Office?

Christopher Graham: If Mr Ellis was here he would find this hard to believe, but I am not looking for work.

Mr Brown: He is not here, tell us what you really—

Christopher Graham: I am very happy to leave that to the Home Office, of course. The Information Commissioner's Office is involved with a lot of liaison with other data protection authorities across the European Union and elsewhere, and we are active in our work in the Article 29 working party on the revision of the data protection regulation. I am off to the international conference at the end of the week to liaise with the Americans, the Australians, the New Zealanders and practically everybody else, because this is a global business that we are in and it is no good having a regime that works just in the UK, particularly if you need to retrieve fugitives from Bordeaux, for example.

Mr Brown: Do you think these arrangements work well or have you just not formed a view? If you are a public authority that used the powers that they have but rarely, is this a reasonable route for them to go?

Christopher Graham: I should not stray into a territory I do not know an awful lot about. It has not come across my desk. The mutual legal assistance scheme has not come across my desk.

Q711 The Chairman: Finally, or penultimately, commissioner, you have just said that you are involved in international discussions with your international colleagues. If this Bill were to go ahead, would the UK be in a unique position with these proposals—unique in the technological side and unique in the level of data gathering and intrusion?

Christopher Graham: I know that the data retention directive has run into a lot of trouble in different jurisdictions in the courts, and that was just the previous data protection directive, so I do not know how this would fly. We are assured by the Home Office that it is compliant with the Human Rights Act. I am sure there will be lots of people queuing up to challenge that, but that would have to be seen.

The interesting thing is how this whole area plays out at the moment, because we have very complex negotiations on the regime that will replace the current Data Protection Act, which follows on from the data protection directive, which is in the process of being reviewed. It looks as though we are going to get a regulation instead of a directive: in other words, something will just apply directly, as you know, without the need for transposing everything except police and justice, which is or is not going to be subject to a separate, new directive. I wish it was possible to have a clear set of rules that just applied to all data protection activities in whichever sector. I cannot believe that it is a good idea for police forces to have to conduct some of their work under the new proposed regulation and some of their work under the new directive, if there is a directive, but that is probably an argument for another place.

The Chairman: But that directive might have less stringent requirements than the general regulation, which could result in some member states lowering standards. Would the UK be one of those states with lower standards?

Christopher Graham: There are differences of opinion around the table in the Article 29 working party on where the regulation that applies to everything apart from police and justice is unacceptable because it set standards that are too high and too rigorous or that it is unacceptable because it set standards that are less than the standards that are enjoyed in many member states.

In the case of policing, it is important to make clear that the proposed directive would not, as I understand it, affect domestic policing. It would affect only the transfer of information across the borders and so on.

The Chairman: Thank you very much. Any other final questions?

Q712 Lord Strasburger: Just one question. Coming back to encryption and CSPs that are not within the system, is it possible, in your mind, that the implementation of this Bill could have the opposite effect to the one that is intended and that when the bad guys have moved to encrypt their information and to avoid the ISPs that are being monitored, the public authorities end up with access to less data than when they started?

Christopher Graham: I suppose that that is a hypothetical case that you are advancing, and I hope that nothing I have said this afternoon has made that more likely. On the other hand, it is just in the nature of things. That is the way in which things will go. The questions then arise: what resources are going into this; how much are those communications service providers who are identified going to have to be paid to do this task; how much is the Information Commissioner going to have to be paid; how much is Sir Paul Kennedy going to have to be paid; what is the total

cost of doing something that may be of marginal benefit at the end of the day? Those are questions that I am very glad to leave to you people to decide.

Q713 The Chairman: Sorry for prolonging the session but I have one final point. Your discussions have provoked me. As parliamentarians we always want to pass a law that will last for a long time. As Ministers we know you get one shot at a bit of legislation every five or 10 years. There is a hope here that if the Bill seems to be drafted to a certain width, it will stand the test of time, but is that—and I do not want to put words in your mouth—a rather naive view of legislators? When the technology is moving so rapidly, is it possible for us as parliamentarians to pass a RIPA mark 2 2012, which will last to 2020 without being fundamentally wrong?

Christopher Graham: I think that a confident Parliament would nevertheless include a commitment to post-legislative scrutiny after five years or so, not just because the technology is changing but because you want to see how it works out in practice. I think that is a good thing to do, and it is one of the assurances that Parliament can give to a concerned citizenry when we are dealing with these surveillance matters that we will look and see how it works out in practice as well as in theory.

So I do not think you convince anyone if you say, “The laws that we pass are so wonderful, so we will not look at them for 20 years”. I think Parliament will say, “We have gone through a thorough pre-legislative scrutiny. We have heard all the voices. This is what we think. This is what gets passed and we check how it is going in five years”.

The Chairman: Thank you very much, Commissioner. It has been a long session. We all thank you once again for your excellent written information. The surveillance road map is particularly interesting. I think we all learned from it, particularly that we are going to have new commissioners for cameras and surveillance and other things,

which some of us were not quite aware of. Thank you very much for the written evidence and for your participation today. It has been a long but very worth-while session, and keep up the good work. We cannot make promises on resources, with or without Mr Ellis here, but good luck on what you do.