UNCORRECTED TRANSCRIPT OF ORAL EVIDENCE To be published as HC 479-i

HOUSE OF LORDS

HOUSE OF COMMONS

ORAL EVIDENCE

TAKEN BEFORE THE

JOINT COMMITTEE ON THE DRAFT COMMUNICATIONS DATA BILL

DRAFT COMMUNICATIONS DATA BILL

TUESDAY 10 JULY 2012

RICHARD ALCOCK, CHARLES FARR AND PETER HILL

Evidence heard in Public Questions 1 - 96

USE OF THE TRANSCRIPT

1. This is an uncorrected 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. Any public use of, or reference to, the contents should make clear that neither witnesses nor Members have had the opportunity to correct the record. The transcript is not yet an approved formal record of these proceedings.

3. *Members* who receive this for the purpose of correcting questions addressed by them to witnesses are asked to send corrections to the Committee Assistant.

4. *Prospective witnesses* may receive this in preparation for any written or oral evidence they may in due course give to the Committee.

Members present:

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

Examination of Witnesses

Richard Alcock, Director of Communications Capability Directorate, Home Office, **Peter Hill**, Head of Unit for Pursue Policy and Strategy Unit, and **Charles Farr OBE**, Director General, Office for Security and Counter-Terrorism, Home Office

Q1 The Chairman: Welcome to this afternoon's session. We begin our first public evidence session with officials from the Home Office. Welcome, Mr Alcock, Mr Farr and Mr Hill. Perhaps, gentlemen, I could ask you to introduce yourselves and say what your role and function is and then I will ask if you wish to make any opening statement before we begin the questions session.

Peter Hill: I am Peter Hill. I am the Head of the Pursue Policy and Strategy Unit in the Office for Security and Counter-Terrorism. Among my responsibilities is oversight of the policy and law in relation to covert powers, including communications data.

Charles Farr: Hello. My name is Charles Farr. I am Director General of the Office for Security and Counter-Terrorism.

Richard Alcock: I am Richard Alcock. I am the Director of the Communications Capabilities Development Programme.

Q2 Michael Ellis: Mr Farr, the previous Government enacted pieces of legislation that affected the area of communications. I am referring now to the Regulation of Investigatory Powers Act—RIPA, as it is sometimes referred to. What are the key facts that lead the Home Office to believe now that powers in this draft Bill, the Communications Data Bill, are necessary?

Charles Farr: One aspect of RIPA, as you know, concerned the access which public bodies may obtain to what we call "communications data", which we understand, and you know this very well, to include information about a communication—of course, not the content of the communication itself. In that particular area, RIPA, to some degree, has been overtaken by technical change in the communications industry and changes in the way people use communication, with the result that the data that public authorities have had access to in the past is no longer as readily available to them as it used to be, for a variety of reasons that I am happy to go into now if you would like me to do so.

Q3 Michael Ellis: Perhaps you could elaborate.

Charles Farr: The change in communications usage is, very simply, one that involves a shift from mobile phones of an old kind, if I can put it like that, to computer-based

communications. As that transition has happened, so have two or three other consequences of it. First, communications service providers—CSPs, if you will—no longer retain, for their own business purposes, communications data as we know it. Indeed, sometimes not only do they not retain it, but they do not generate it either. Therefore, when public authorities seek access to that data, on a case-by-case basis, there is nothing to which they can get access, because it is not retained by the provider.

Q4 Michael Ellis: So, previously, say 30 years ago, BT may have kept data because they needed it in order to bill people correctly.

Charles Farr: Yes.

Michael Ellis: But today, data is not kept in the same way, so if you were to seek relevant information, the service providers would not necessarily be able to provide it.

Charles Farr: That is correct. So, in the old days of a single telephone line in your home or office provided by, pretty much, a single provider, that single provider required quite a lot of communications data to enable the provider to bill you appropriately on a call-by-call, duration-by-duration, destination-by-destination basis. As we move from the world of old-style telephony to the world of computer-based communication, that business model ceases to apply. I suspect many people in this room will have experienced this; you no longer pay per transaction, if I can put it that way, or per communications event. You pay per month or per year.

Q5 Michael Ellis: You pay per month to have a broadband service rather than per call.

Charles Farr: Yes, and the provider has much less interest in aspects or some bits of data than used to be the case. I think the provider will, very often, obviously be interested in your subscriber identity, if I can put it like that—who you are and where you are—for billing purposes, but may not be interested in very much else, in fact.

Q6 Michael Ellis: So, Mr Farr, is it a correct characterisation that the Home Office is seeking not to extend powers deeper into the area of privacy but simply to prevent a further degradation of powers that were previously available and that you say are declining?

Charles Farr: It is certainly true that a capability gap, if I can put it like that, has opened and public authorities can no longer get access to the data that they would want. As you know, we have put, based on our survey of the relevant organisations, a figure of 25% of data that organisations would like to get access to but cannot.

Q7 Michael Ellis: Can I press you on that 25%? How much of that 25% that you can now no longer obtain is due to non-compliance by the communications service provider and how much is simply not available because those CSPs do not have the data?

Charles Farr: I do not have the exact proportions, but in large measure it is because the data is no longer available. Sometimes it is also because the legislation under which we are operating, RIPA, but in particular—I am afraid this is where it gets more involved—the data retention directive, is not clear about what data the provider should retain even where the provider has retained it and could, in theory, retain it if the provider chose to do so. So there is, if you like, a technical problem, which I have referred to already, lack of data; that is then compounded by a legal problem that the EU DRD, the governing legislation on retention, is not very clear about what IP data, computer-based data, the provider should retain as well. So you are hit by two issues and both of those affect the capability of public bodies to get access to the data they need.

Q8 Michael Ellis: If the DRD is not clear, does that not also operate as a negative in the other direction, in that service providers could retain information for longer than would be required, for example, or longer than they should do?

Charles Farr: I think the ambiguity in DRD is certainly making for a variety of different practices across countries in Europe which have transposed DRD, which is almost all, and there are different interpretations by those countries of what companies should retain, particularly regarding IP data. I emphasise that on mobile telephony of an old kind and fixed-line telephony the DRD is much more specific. So, to that extent, the answer to your question is yes.

Q9 Michael Ellis: Is there evidence that the changes proposed by this Bill would make available the data requested in that 25%?

Charles Farr: Yes. As part of the business case that we do—Richard is responsible for that and it comes through me—it goes first to the Home Office Business Board, then to the Treasury and to other departments. We have to make, obviously, a really detailed business case explaining how much this is going to cost, what benefits we might accrue from it and, of course, the technical feasibility. We are clear that the measures proposed in this legislation would, first, stabilise the degradation and then, over a period of time, improve our coverage to a figure of what we think should be in the region of 85%, as opposed to 75%, which is where we are now, probably over a period going out to 2018.

Q10 Michael Ellis: On the subject of the communications data that is currently used, we are told that under RIPA—this is the pre-existing legislation; it is legislation that has been on the statute book for some years—in 2010 there were over half a million requests for communications data: 552,550. Could you elaborate on what a single request can comprise of? Would one of those half a million requests cover more than one person and would the investigation of one person generate more than one request?

Charles Farr: There is a group of questions in that; let me try to unpack it as best I can. First of all, a single request for data can be for more than one item of data. Let me give you an example: requests are about instruments, not people, for the simple reason that, generally speaking, you may not know who owns an instrument before you seek the data from the instrument concerned. When you request data about that instrument, that communications instrument, you might request both the subscriber and, perhaps, whereabouts that instrument was at a particular time on a particular day. So a request regarding a specific instrument may elicit and be intended to elicit more than one item of data about the instrument in question. Is that clear?

Q11 Michael Ellis: Yes, but could an inquiry relate, therefore, on more than one occasion to the same instrument?

Charles Farr: It is certainly possible that over the course of a criminal investigation—and, as you know, 99% of requests for data are from the police or the security agencies in the context of an investigation, criminal or otherwise—more than one request could be made about the same instrument seeking different information about it, because it may appear, as a result of the first data request, that that instrument is important and clearly centrally relevant to the investigation. At that point, the investigator may well feel it is both necessary and proportionate, which are the two criteria that will be in his or her mind, to go back in and get more data, so yes.

Q12 Michael Ellis: So half a million requests for information or for communications data does not represent half a million people.

Charles Farr: That is certainly true, because many of the people who are under investigation in a criminal investigation will use numerous telephones, or instruments I should say—it is not just telephones—at once and dispose of them very regularly. So it might be that a single person, over the course of an investigation lasting three months, gets through 30 or 40 different instruments, all of which generate, for the investigator, different requests. So it is certainly true that 500,000 requests do not equal 500,000 people. It is very hard to come up with a figure about how many people they do relate to and we are doing some more work on that in an attempt to better inform you.

Q13 Michael Ellis: Perhaps you would let us know that figure, if you can.

There was a snapshot survey in 2010 by the Home Office, which indicated that 17.3% of police communications data requests were for non-serious crime. Could you say something, Mr Farr, or one of your colleagues, about what is meant by "non-serious crime"? Further to the points you were just making, for example, do you know, in the average murder investigation, how many data requests there might be and relate that to what is meant by "non-serious crime"?

Charles Farr: If I can take the second question first, in an average murder investigation it is difficult to come up with an average figure, but from the work we have done it is very possible that the number of comms data requests could be between 500 and even 1,000. Generally speaking, in a murder investigation they may just be for subscribers, in the first instance, trying to find out, very simply, who a victim has been in contact with in the preceding year, a year being the outer limit for the time for which data is being returned, at least under DRD. So, yes, a single investigation can create a lot of data for a single—

Q14 Michael Ellis: What about the non-serious crime?

Charles Farr: There is no single statutory definition of "serious crime", unfortunately. That complicates my answer to your question, but non-serious crime could include, for example, in this particular context, harassment, stalking, aggravated theft, assault on a police officer, and some aspects of fraud. All of them could well be non-serious crime.

Q15 Michael Ellis: So perhaps crimes that would be dealt with in the magistrates' court rather than the Crown Court.

Charles Farr: They could be, yes.

Q16 Michael Ellis: How many of the half million requests were not for criminal investigations at all? Do you know that?

Charles Farr: 99% of applications for communications data are made by the police or the security services. Not all of those, of course, are made in the context of a criminal investigation. A proportion, I think, from recollection—my colleagues may have the information in their head—but somewhere around 6% or 7% are for missing people and people at risk and in danger. I am just checking my figures: 5.65%. 1% of communications data only is used by or represents applications by organisations other than the police and the agencies. Of that 1%, the two biggest chunks are local authorities, one, and the Financial Services Authority, two. The types of data that local authorities get we can then talk to you about or send you the details of, if you wish, but most local authorities' requests for data are for subscriber data; it is well over half.

Q17 Michael Ellis: Is this for such things as benefit fraud and the like?

Charles Farr: Yes. Local authorities may use simple forms of communications data, if I can put it that way, to investigate those crimes—generally less than serious crimes—for

which they and not the police are responsible. That could include, certainly, benefit fraud, trading standards crime, and some antisocial behaviour as well.

Q18 Dr Huppert: Firstly, Mr Farr, can I apologise? I am going to have to leave shortly to present a Bill in the Commons. I just have two, hopefully, quick questions, if I may. The first one is just to understand the scope of a request. How broad could a request be? Could a request be, for example, to get all the information from every subscriber to a service for a period of a week? Would that be possible within the current law?

Charles Farr: No.

Q19 Dr Huppert: That is very helpful. My second question is about the other serious crimes that Mr Ellis was referring to. The Chief Constable of Derbyshire, Mr Creedon, who is the ACPO lead in the area, said last month that he would consider it perfectly appropriate if he saw somebody texting or using a mobile phone while driving to use the communications data for that. Is that the sort of thing that you and the Home Office would envisage this being for as a non-serious crime?

Charles Farr: I think it is fair to say that we do not think that use would be central to this legislation, and this legislation clearly has not been planned with that in mind. That being said, it is common practice, in the event of a fatal car accident involving fatalities, for communications data to be obtained to try to understand whether the people involved in that crash have been using telephones at the time of the crash itself. So, to that extent, yes, but I would not want to overstate it at all.

Q20 Dr Huppert: Mr Creedon was implying it would be a standard use when you saw somebody driving along using a phone. You would not accept that?

Charles Farr: I hesitate to contradict Mr Creedon. I think you would have to demonstrate necessity and proportionality; let me put it like that.

Peter Hill: The figures certainly do not bear that out.

Q21 The Chairman: Are you, therefore, worried about function creep? That is, you give the police or the security services the power to deal with terrorism, serious crime, paedophiles—the high-level stuff—and within minutes of the Home Secretary's announcement at the press conference, Mr Creedon was suggesting that speeding motorists ought to be caught as well. Does that concern you, the general point about function creep?

Charles Farr: I think the application process used by the police to get hold of communications data, in my experience and our experience of it, is a thorough and really serious bit of work. The applying officer has to seek authority in written form, justifying the request on the grounds of its necessity for the investigation and its proportionality to the office that is being committed. That application has to consider collateral intrusion, the degree of innocent persons' data that is going to be acquired. That has to be signed off by a senior officer in the police force, a superintendent or an inspector, and it has to be verified by what we call a single point of contact—inevitably the acronym is SPOC.

Q22 The Chairman: I accept all of that, Mr Farr, but speeding motorists are a far cry from terrorism, serious crime and paedophiles.

Charles Farr: If we look, Mr Chairman, with permission, at the work we have done more recently on the use of communications data, I think it does bear out my point that speeding motorists really do not figure on the list. 27% of data for which applications are made and obtained is for drugs-related offences, 15% is for property offences, arson, armed robbery, theft, 12% is for financial offences, 10% is for sexual offences, 6% is for homicide,

5.65% is for missing persons, 5% is for harassment, 4% is for offences against the persons, and 4% to 5% is for explosives. Speeding is not mentioned.

Q23 The Chairman: So you would be happy to see the Bill toughened up then in terms of proportionality, or some of these cases excluded.

Charles Farr: Your Committee will obviously have a view on that. I think that the police process for determining necessity and proportionality is an effective one, but you will obviously come to your view on that.

Q24 Lord Armstrong of Ilminster: I can understand that the police might want to know whether a motorist has been using his mobile phone if that was thought to have led to a fatal accident in which somebody was killed. I would have more doubts about it if it was just looking after speeding motorists where there was no such event. I wonder if you could comment from that point of view.

The other question is you said just now that there is no definition of "non-serious crime" and I understand that, but in other contexts people have used the length of minimum sentence as a definition of non-serious crime and I wonder if that could be used in this instance as well.

Charles Farr: You are absolutely right, of course. Perhaps I could just ask, with your permission, if Peter could comment on that. We went through a process of looking at definitions of serious crime for the Government in the context of the review of CT powers, you may remember, in January last year.

May I just come back to the speeding motorist? I emphasise that an applicant from the police service has to demonstrate necessity and proportionality, otherwise the application will not be approved. Applications are refused; the Interception of Communications Commissioner's report, due out next week, will give a number, I think for the first time, of applications which are refused. If the necessity argument is not made out, and I personally find it hard to envisage circumstances where speeding per se would require communications data, then the application will not go through. That will then be reviewed, as you know, by the Interception of Communications Commissioner, who will look at the requests and determine whether, indeed, the test of necessity and proportionality have been met. I understand the concern. I do think the arrangements that are in place should address it.

May I just ask Peter to comment on the serious crime question?

Peter Hill: Two quick points. The first is on the data that you referred to, the 2010 survey. First, I think it is worth bearing in mind it is a two-week snapshot, so it is an indication, no more than that. Second, there are shortcomings in that, in that there is no definition or indication of what the people reporting in the survey defined as serious versus non-serious, so that is its limitation. In the study that we are conducting now, and that we hope to let you have data on later this month, we avoid that by simply listing the offences under which data is being requested. That should give a much more detailed picture of what this communications data is being used for.

Secondly, you are absolutely right. There is no single definition of serious crime on the statute book. There are a number of definitions, some based on a list, some based on a tariff. One could introduce, as you say, a minimum threshold. I think the two issues you might want to consider there are: what is the threshold and what falls below it? For example, under most definitions based on a custodial sentence, something like harassment or stalking, which are communications crimes, would not meet that criterion and yet they can have an absolutely incredibly damaging impact on the victim, and, of course, they can escalate into far more serious crimes. We know of cases where that sort of harassment—40 or 50 phone calls a day, stalking someone in the street—does turn into a far more serious crime. So you would have to

somehow find a way of managing that investigative process whereby you start with a less serious crime and end up with a very serious one. That is not to say it could not be done, but you would obviously lose the ability to use the information for a number of crimes that either people consider quite important or have the potential to lead to the investigation of more serious crimes.

Q25 Lord Armstrong of Ilminster: It was once said by a Metropolitan policeman that in Devon and Cornwall bicycle theft was serious crime. Can we be reasonably confident that bicycle theft would be excluded for the purposes of this legislation?

Charles Farr: Yes.

Q26 The Chairman: If I may follow up on Lord Armstrong's point, I think he is making a point of principle that it is not just bicycles, but less serious crime. Would you, in certain circumstances, if we could get the definition right, be willing to dump the less serious crime part out of the Bill?

Charles Farr: I think Peter has talked to the issue. I suppose the question is: less serious crime from whose perspective? If you are being harassed with 50 telephone calls a day and you have a legitimate fear of subsequent assault, I do not know whether you would consider that to be such a less serious crime that it would justify the police, under any changes to this legislation, not having access to the data that could resolve the threat you face. I would feel uncomfortable with that.

Q27 Lord Armstrong of Ilminster: I can think of trying to exclude less serious crime unless it became part of an investigation where that was thought to be incidental to a more serious crime, which I think was something that you foreshadowed in your previous answer. I just wish to see if there is any future in going down the road of an exclusion of less serious crime unless and until there is evidence to think, or reason to think, that it might be part of a more serious crime.

Peter Hill: I am sure you will have police officers here shortly and you will want to ask them about that. The only point I would make is that the feedback we get from them is that it is often the investigation of the less serious crime that leads to knowledge of a more serious crime, and it is often through the investigation of apparently more minor offences that people who one believes are engaged in more serious criminal activity can be approached. But I am sure those are questions that you will put to the CPS and to the police.

Q28 Lord Strasburger: Going back to your 25% shortfall of information you cannot get your hands on, what proportion of that 25% gap is due to customers choosing to conceal either their identity or their activity, either for nefarious reasons or perfectly innocent reasons?

Charles Farr: Richard may want to comment on that, but perhaps I can just say a few things. I think the answer to that is not very much. If you have the data provided for in this legislation, then you can resolve increasingly anonymous communications, which are a feature of the communications environment in which we live. To put it another way, if you have the right kind of data, issues of anonymisation cease to be a significant problem.

Q29 Lord Strasburger: So is there any risk, if this Bill is enacted, that those with a good reason to conceal their identity or their activity, or those who just choose to do it, will make greater efforts to do so and your gap will reopen?

Charles Farr: If people choose to take greater efforts at anonymisation, that is not necessarily a problem for this Bill. If they are engaged in a criminal activity that we are investigating, then of course, in theory, it may become a problem. I am satisfied that with the

techniques that are being developed, which will be facilitated by retention of a kind envisaged in this legislation, many workarounds can be defeated. However, one point I would emphasise, and perhaps I can do it now—I could have done it earlier—is that we are not proposing this legislation on the grounds that it will recover 100% coverage of the communications environment. Those days have gone and you will note my earlier comment that we are not seeking or anticipating that they will return. So there will be cases, of course, where people can find, perhaps temporarily, workarounds to some of what is envisaged here, but I emphasise we still envisage that by 2018, with this legislation, we can stem the capability gap and restore coverage to somewhere approaching 85% of what we need.

Q30 Lord Faulks: Just going back, briefly, to the notion of serious crime, I do not think anybody is concerned with what you might call trivial crime, but is there not a danger if you start defining serious crime, which is essentially rather a subjective concept anyway, that you are potentially going to prevent exactly what you want to achieve, that you already have the safeguards provided by necessity and proportionality and that we would be searching for a chimera by trying to better a definition of serious crime?

Charles Farr: I think that is our view and I think that the concern about the trivialisation of the use of communications data is therefore better tackled through an examination of the application process and the extent to which necessity and proportionality are, indeed, ingrained in the system. That feels, to me, a more likely route to avoiding trivialisation than defining or redefining serious crime, which, as you rightly say, is fraught with hazard. I personally believe that the necessity and proportionality tests are met by the users who use most of this data—the police—but you will come to a view on that.

Q31 David Wright: I am interested in the point you were making earlier about criminal networks or individuals using 20 or 30 or 40 devices. I think one of the concerns people have is that, in order to target this, there is a danger that you would go on a fishing expedition, looking at devices in an area. It is very difficult to pin those devices down to an individual. How do you hone down your investigation? This may be on very serious crime, the other end of the spectrum to some of the lesser crime we have been talking about. How do you ensure that you are targeting the activity properly of those individuals and we are not out on a fishing expedition that captures thousands of other people's data?

Charles Farr: I am going to sound a bit like a long-playing record. The investigator has to demonstrate to the senior officer that those instruments for which he or she is seeking to obtain data—be it a subscriber, usage data or traffic data—are centrally involved or connected to a criminal investigation. Now, clearly, he or she is going to use all the skills and abilities that they have and, indeed, the training in this—and there is quite a lot of training we provide already—to try to home in on those devices that are more than normally employed. That will be an iterative process. Try to find the phone that is making the most calls, that is most active, which is most closely in contact with the person or people who are at the centre of the investigation and, by a process of elimination, work towards greater amounts of data on the instruments that appear to be focal points. So I think at every step you demonstrate necessity, you demonstrate proportionality and you work your way towards those instruments that seem more than normally important. I cannot give you much more of an answer on that. Peter or Richard may want to add to it.

Q32 The Chairman: Finally, before we leave these 552,000 requests, could I be clear in my own mind? You are suggesting that that does not relate to 552,000 people. That would be an exaggerated figure. It would be likely to be many fewer people.

Charles Farr: No, not likely; it will relate to many, many fewer people, of that there is absolutely no doubt.

Q33 The Chairman: So one request could relate to more than one person. I am putting it the other way around.

Charles Farr: In theory, yes, because a request might be for an instrument that is certainly connected to more than one person.

Q34 The Chairman: Generally, you are saying that there could be 1,000 requests, but that might relate just to one or two people.

Charles Farr: It could certainly relate to an organised crime gang of, say, 10 people.

Q35 The Chairman: I understand. Are you aware of any circumstances then where the reverse applies: where there could be one or two requests that might relate to 100 or 1,000 people?

Peter Hill: I do not know the details of the applications made by individual officers, but of course they will always have to demonstrate necessity and proportionality. I am trying to think of where one request might cover hundreds of people.

The Chairman: Or thousands.

Peter Hill: I struggle to think of the circumstances where that may apply. What I could think of is, for example, the phone of a murder victim. You want to find out all the calls received by that individual in the hours running up to their death. That could be a significant number of people.

Q36 The Chairman: I will not press you today on this, because we must move on, but I would be grateful if you would do a check back to see if there are any circumstances where one request could relate to hundreds of people or subscribers, or thousands of people.

Charles Farr: I am with Peter. We will obviously do what you want. I cannot see the circumstances. Sometimes it is the case that a single instrument—a single telephone or laptop—is shared among a criminal network, even a terrorist network, because that instrument is regarded as being safe and secure and, therefore, is used by a number of parties, but not to the scale that I think you may be concerned with.

Q37 The Chairman: There would never be circumstances which critics of this Bill would call a fishing expedition where you get a couple of access requests for thousands of people.

Charles Farr: No.

The Chairman: Excellent.

Peter Hill: One area I think we will look at for you is whether, for example, in a serious terrorist investigation one is trying to locate an individual who was in a number of places at certain times, and you then try to get the information from those cell sites in order to work out which phone was in those places at those times. Obviously, that could require you getting a large number of individual bits of data, to work out which phone was in those bits at the same time. The Bill, just on that point, does have a mechanism which is intended to help reduce the amount of data that the law enforcement agencies would acquire in that context. Rather than needing to get the information from each location, they would ask which phone was in each location, and then the filter would do all the work for them and just give them the information they needed. So the Bill does have a mechanism in it to try to reduce, in those circumstances where large volumes of data might be requested, that volume of data to the

minimum that is necessary to answer the question. But I think it is certainly something we can come back to you with.

Q38 The Chairman: I think we would like some more information on that in due course.

The Home Secretary said, in letters to Members of Parliament and to Peers, and it was the main justification for the measure, that this was necessary on the grounds of national security, detecting serious crime, the economic well-being of the nation and tackling paedophiles. Yet in the draft Bill, Clause 9(6), we have about 10 purposes listed, including public safety, public health and, rather than just the economic well-being of the nation, we have collecting any tax, duty or levy, and things that may damage a person's physical or mental health. So we are being told the Bill is necessary for large and important reasons of national security, terrorism, serious crime, and yet are you are concerned that part of the Bill has a lot of extra material?

Charles Farr: Clause 9(6), which you are referring to, simply, with one exception, transposes purposes that are set out in RIPA. The single exception to that is Clause 9(6)(c), which says, if I may read it, "for the purpose of preventing or detecting any conduct in respect of which a penalty may be imposed under section 123 or 129 of the Financial Services and Markets Act 2000 (civil penalties for market abuse)". That was added because it had been removed from another piece of legislation that had hitherto been used by authorities to get access to communications data. So having removed it from another piece of legislation where it had facilitated access to data, it was replaced here.

On this list of purposes, Chairman, as you say, it is long. I think it is fair to say, as the Home Secretary pointed out, the vast majority of requests for data are in relation either to "a) in the interests of national security" or "b) for the purpose of preventing or detecting crime or preventing disorder" or "e) in the interests of public safety". It is true that a number of others have been added in, and I am sure you will want to look at those and we will try to give you as much data as we can about the extent to which they have been relevant to particular requests.

Q39 The Chairman: Would you accept that, to a certain extent, it does fuel the suspicions of those who are opposed to this Bill that we hear it is for essential purposes—preventing terrorism, serious crime and paedophiles—and yet the list of purposes has a much wider range?

Charles Farr: I am looking at the list of purposes in front of me. Some of them seem to have a really narrow range: "9(6)(j) where a person (P) has died or is unable to identify themselves because of a physical or mental condition, (i) to assist in identifying P, (ii) to obtain information about P's next of kin" and so on and so forth. In other words, I am not sure that the large number of purposes to which you rightly allude, beyond those core to which the Home Secretary referred, are very expansive. I think rather the opposite: some of them are very specific and somewhat esoteric.

Q40 The Chairman: In that case, would you be averse to a warrant system for applying in those circumstances? If there are very few requests, then why not go to a magistrate for a warrant?

Charles Farr: I think, given that the numbers are likely to be very low, then technically, logistically, clearly that would be feasible. You will come to a judgment about whether the oversight that a magistrate could exercise—going back to our mantra of necessity and proportionality—is really going to be more effective than the oversight that might be exercised by other authorities, but I accept that there is a case, yes.

Peter Hill: If you look at some of the purposes, they are purposes for the preservation of life. They are to find missing and vulnerable people. They are often requests for communications data that are made with great urgency in order to locate somebody. Whatever system one has in place, you will clearly need something that allows you to have an urgent procedure to access the data, and 5% or 6% of data requests, as Charles has said, are for that purpose.

Q41 The Chairman: Yes, I accept that, but there are others which are clearly not of an urgent nature. When you were drafting this Bill, did you consider in the Home Office, because of the history of trying to get to this stage in the past, drafting the Bill more tightly, so that it only did include serious crime, terrorism and national security issues?

Charles Farr: Yes. We certainly looked, I think it is fair to say, fairly exhaustively at a very wide range of options. I think ultimately what persuaded the Ministers to leave it as is was that the vast majority of requests are for "a) in the interests of national security, b) preventing or detecting crime or preventing disorder" or "e) in the interests of public safety". Those others seem to have been shown to be necessary in very specific cases, but have not collectively created a significant number of requests. Therefore, if they can facilitate, on occasion, specific investigations they should remain in the Bill, but I am sure your observations on this will be understood.

Q42 The Chairman: Finally from me in this section, would you be able to give us a breakdown of the data requests per purpose? So would you be able to give us a breakdown of the data requests relating—I understand you may not wish to do so for national security—to preventing and detecting crime, public safety, public health, and all the categories in 9(6) and can you tell us if there are any which have never been requested?

Charles Farr: As I alluded to earlier, we have two pieces of data on this which are relevant to your question. One is a bit of research that was done in 2010 to look at police applications for data under the crime types that they were investigating. The second was a repeat of that bit of work, which we will finalise in the next few weeks and give to you, of course, which again has taken a snapshot around the country over a two-week period of the crime types in connection with which applications for communications data were made.

The tricky bit is that the categories that we have used to indicate for what crime types data has been applied do not correlate one-to-one with the purposes set out in 9(6). We can tell you, and I specified it earlier, what percentage of communications data has been requested in connection with missing persons and abandoned 999 calls. I have said already 5.6%. That, I think, is what I would understand to be a part of the public safety component.

If I may, we can write to you with our survey, mapping wherever we can the survey on to the purposes and I think that will answer your question.

Q43 The Chairman: That would be helpful and, if you can widen it beyond the police into the public health and the other aspects, the other purposes listed in 9(6), that would be helpful.

Charles Farr: We will do as much as we can.

Q44 Baroness Cohen of Pimlico: Along the stretch of the Bill, what comes under the term "communications data" as drafted? Would it capture a web activity log, for example? There is a suggestion in the media you capture the content of a postcard, which perhaps you cannot have intended. What is your view about what is the stretch of communications data?

Charles Farr: I can deal with the second question very easily. It does not capture the content of anything, a postcard or an e-mail. So that claim is incorrect.

Baroness Cohen of Pimlico: It did sound strange.

Charles Farr: It is strange and it is not in the legislation. On web logs, or web activity logs, as they are called, yes, communications data does capture information demonstrating or indicating the websites to which a device has connected. It does not then enable a public authority to see what has happened within that website unless a communication is involved. Let me try to put it in another way, if I may. Communications data will show which website you have accessed and will show a communication, if you have made a communication using a website. It will not otherwise show the pages of the website or other aspects or parts of the website that you may have visited simply as a reader.

Q45 Baroness Cohen of Pimlico: To use my simple-minded example, I am a regular user of the Ocado website, so the data will reveal that.

Charles Farr: Yes.

Baroness Cohen of Pimlico: But not the contents of my grocery order.

Charles Farr: No.

Q46 Baroness Cohen of Pimlico: Is there anything else I have not thought of that communications data, in fact, spreads to cover? Web activity logs I think one might have thought of.

Charles Farr: I should say, by the way, that this legislation does not change the definition of "data" in respect of web activity logs. It already was accepted in the definition of "communications data" that communications data includes web activity or web logs. There is no other respect in which the definition of "communications data" has changed in this legislation.

Q47 Stephen Mosley: When it comes to cryptic communication, for instance, SSL or something, the encrypted communications data might be in the content of that communication. How is that classified?

Richard Alcock: Through the Bill, we will only be able to store communications data. The means by which we access communications data, our preferred route, will be working in partnership with the communications service providers, who will hold unencrypted data on their own services, i.e. the services that they are providing for their customers. We will be working with them to retain, in some cases, some aspects of communications data and, in that case, it is very easy to separate content from CD. Though I must stress, through the Bill it is illegal for us to collect content. We will only be able to retrieve and store communications data. We will not be applying any systems that cannot reliably extract CD from content through whatever data streams. So, in essence, by working with communications service providers, we can ensure a very reliable means by which we can ensure that we only collect communications data and store that appropriately.

Q48 Lord Faulks: I want to ask you about overseas CSPs, or rather CSPs that are based overseas. Technically, the Bill extends to them. How realistic is it to pursue them for potential breaches of duty?

Charles Farr: If I may, before we get to the question of how realistic, I suppose the prior question is whether that is going to be an issue at all. We have already, of course, relations with many, but by no means all, overseas providers, including those who are household names and are the big suppliers into this country. We have that relationship, for all sorts of reasons, under existing legislation. Those relationships are co-operative and collaborative and, as some of those providers have made clear, they provide data, to the extent that they can—I would emphasise that—in accordance with existing legislation. It is our hope

and expectation that that collaborative relationship would continue and it would be part of the purpose of this legislation to facilitate that wherever we can.

You are right, however, that the obligations do apply to overseas providers and in the event, which I regard as unlikely, that co-operation was not possible, an enforcement route would be open to Ministers, if they chose to exercise it, through civil action. This would apply as much to overseas providers as to domestic providers. I emphasise that is not the purpose of this legislation. The purpose is to facilitate a collaborative, co-operative relationship, building on the relationships that we have already.

Q49 Lord Faulks: At the moment, what percentage of requests for communications data from overseas-based companies are complied with currently?

Charles Farr: I do not have a statistic. We can—

Lord Faulks: Can you give us an idea, please, of the degree of collaboration and co-operation?

Charles Farr: Peter, do you want to touch on some of the issues there?

Peter Hill: Just in terms of framing the answer, the request may not be the best measure, because under the regime we operate, generally speaking, you should not be making a request if you do not believe that the data is going to be there. So, generally speaking, we will expect most requests to be met. The issue that we have is that requests are not made, because people—the single points of contact in the public authorities—do not think the data is going to be there, so there is a self-censorship in requesting internet-related data. They do not think the data is there, either because it is not retained or because it is not retained in the form that they need it and, therefore, they do not request it. So, generally speaking, one would expect most of the requests made to be met. There will be some that are not and where there is company policy which means they are not being met, that is what we need to work through with the companies to try to up that level. But the bigger issue is that the data that we need is not available—although there are some exceptions—rather than it is not being shared with us.

Charles Farr: Typically, with overseas providers, it is a patchwork quilt; they all look a bit different. Some overseas providers do not have the data. Some have the data but do not want to disclose it, because they do not think there is a legal basis to do so. Some will disclose it, but only in the most serious instances, e.g. terrorism or other threat to life. Some may disclose it, but not in a timeframe that we are used to and that is needed in the context of a rapidly moving criminal investigation. Some may disclose it, but in a form that is hard for us to make use of. So there are a range of issues presented by overseas providers. I reinforce Peter's point that calibrating the service, if I can put it like that, that we get on the basis of requests met or not met is probably going to give an inaccurate picture.

Q50 Lord Faulks: I suppose breach of duty is rather a blunt instrument, is it not?

Charles Farr: Yes.

Q51 Lord Armstrong of Ilminster: Have you assessed the risk that this legislation might either drive service providers overseas in order to escape the obligations under the Bill or that users of communications equipment might seek to use overseas service providers rather than domestic ones in order to escape observation?

Charles Farr: On the first issue, if I may, we have a dialogue with the major CSPs in this country. We have it for all sorts of reasons to do with communications data and, indeed, interception, which also falls within our responsibilities. That is a really constructive dialogue, because major providers recognise obligations they have to provide data and, indeed, to facilitate interception. This legislation—the principles of it, the reasons for it, and the background to it—have been discussed repeatedly in that group and, insistently and

consistently, we have had the same response: that those providers understand there is an issue here that needs to be addressed. They want to help address it, but they expect there to be legislation to provide a legal basis to enable them to do so. At no point, in my experience, has a major CSP suggested or even implied that they would rather move overseas than work with this legislation.

On your second point, whether people will move, people already do. Criminals and people engaged in criminal activity spend their lives trying to evade systems that we have constructed and put in place, and work that we do with providers, to evade our attention and control, if I can put it in that way. So I do not think the Bill is going to change that; it already happens. I think what this Bill will do is to give us greater ability to manage that problem when we see it.

Q52 Stephen Mosley: One of those abilities, of course, will be the ability to put in black boxes on the network in the UK to look at what is happening on some of these foreign services. Could you explain that a bit, because I think it is one area that people have concerns about? If it is encrypted traffic, of course, even if it is looking at the communications data, it is going to have the ability to unencrypt the content as well. Who would own and operate those black boxes? Would it be private sector communications providers or would it be yourselves or other agencies?

Charles Farr: Perhaps I can go as far as I can and then I will hand over to Richard on the more technical aspects of this.

I just want to be really clear. So-called black boxes—DPI, or deep packet inspection—is not the cornerstone of this programme. It is not a key or the key feature. It is not the central plank of it. The central plank of this programme is a collaborative relationship with service providers in this country and overseas. DPI, black boxes, or whatever other metaphor or language we choose, only come into play in certain circumstances when an overseas provider or the state from which an overseas provider comes, or both together, tell us that they are not prepared to provide data regarding a service which is being offered in this country and which we knew and know is being used by criminal elements of whatever kind. In those circumstances, we have two options. We could, in theory, accept that there will be a communications service here that is being used by criminals to which we cannot get any access or data. That is not the view of this Government. The legislation therefore creates the option, in those circumstances, of putting a black box, using your language, on a UK network across which the data from the overseas provider must move, with the purpose of sucking off that data, under our guidance—"control" is too strong a word—and storing it through that network provider.

To go to your specific questions, we will talk to the network provider in those circumstances, of course. We will work with that network provider on the technology. We will approve the technology that is going to be used. We will approve the programming of that technology to ensure that it does indeed just take data and not content. As Richard has said, the legislation makes it absolutely clear that it would be illegal to take content under the terms of the Bill. The network provider would store the data.

I want to, if I may, get it in perspective. Black boxes, which attract a lot of attention, of course—partly the language—do not and are not the key issue in this Bill.

Richard Alcock: Answering your point about encryption, there are useful elements within an encrypted data flow. There are unencrypted elements, as I am sure you are aware. By the way, the industry use deep packet inspection equipment now, as a matter of course, to look at their networks. They may have deep packet inspection equipment installed right now in the UK to look at performance, look at allocation of services and the like. It may be possible to use existing deep packet inspection equipment, in the encrypted cases, just to look

at that aspect of the data stream that is unencrypted, to establish, if possible, the who, when and where—the communications data elements. As I said before, if we cannot reliably extract CD by that route, then we will not do it.

Q53 Lord Strasburger: Is DPI applied to the entire pipe or to the data attributable to a single user?

Richard Alcock: It would be applied, in extreme cases, to particular services that may be transiting that particular network pipe. So it might be a particular service or application that is flowing in that particular network. It would not be down to an individual. It would not be intercepting an individual's content.

Charles Farr: If I may add, of course the arrangements for public authorities to subsequently get access to that data are unchanged from the norm. In other words, at no point is it possible to go on a fishing expedition into data that has been acquired off a DPI from an overseas provider. You continue only to have case-by-case access under the usual and existing authorisation route.

Q54 Lord Strasburger: So you would require the service provider to filter out the data that did not apply to the individual that you were seeking to monitor.

Charles Farr: It would not really apply, I think. The network provider would take off the network the data particular to the service of concern to us and store all that data. We would then apply to the network provider for specific bits of the data that has been so stored, in accordance with usual practice. That bit of the application process would be fundamentally unchanged from the norm.

Q55 Lord Armstrong of Ilminster: If I may just revert to the question of the communications data from overseas CSPs, you gave us a reassuring answer, if I may say so, about their willingness to co-operate. Is there any kind of measure of those who will co-operate and those with whom co-operation is difficult or non-existent, a percentage measure or something of that kind?

Charles Farr: We are looking at that. I hope that we may be able to give you more information on that as your scrutiny Committee continues its work.

Q56 David Wright: I wanted to touch on the public authorities covered by the draft Bill. My understanding is that RIPA and associated orders outline the authorities that have previously been covered. This new Bill would supersede RIPA in some ways. Why have you not put out a comprehensive list of public authorities that you would want to include under the auspices of this Bill? It seems to indicate, in sections of the Bill, there would be powers for additional authorities to be added in. Could you talk to us around how you have come to the view about what public authorities should have access to communications data?

Charles Farr: I think the Government took the view that there were four users of communications data—they are the biggest users—who should be on the face of the Bill. That is to say: the police, intelligence agencies, SOCA—NCA in due course—and HMRC. You will recall from our earlier evidence that those collectively consume 99% of data requests in this country. The operative issue is, therefore, what you do with those authorities who seek 1% of data. It is quite a small percentage but, of course, quite a large number, still, of requests: 5,000.

The Government has taken the view that those public authorities need to demonstrate, in a sort of zero-based review way, that they have need for the data in this legislation, for communications data, and should make the case for it. We have written to all those public authorities asking them to set out their business case, building on the information that they

have previously provided to us—and, by the way, which we published in 2010 in a RIPA consultation document; we are happy to provide that if you have missed it. We are interested in how often they access CD and why, what alternatives may be open to them, and whether they can provide evidence that they use it in a necessary and proportionate way.

We will then assemble the evidence that we collect from that survey, and we assume you will look at it as well, and the Government will come to a decision.

Q57 David Wright: Will we look at it? You assume we will look at it and that was my follow-up: how is Parliament going to have any oversight on that information? I welcome the fact that you are almost using this process as a review back to see what authorities ought to be entitled to access information. I think that is welcome, but how are we going to have some oversight into that? How can you demonstrate to us what criteria you have used, how it has been assessed, and will that come back before Parliament for affirmative action?

Charles Farr: As we proceed with our review and we get responses from those public authorities, you obviously may wish to talk to us further about what evidence we have received.

Q58 David Wright: What is your timescale?

Charles Farr: Peter will know that.

Peter Hill: I think we are hoping to collate the information that we have asked for by the middle of the summer, so when we are back in the autumn we should know what the business cases are that these public authorities are making.

David Wright: I presume you will be presenting that to this Committee.

Charles Farr: I am sure we will be very happy to. I think we had thought, but of course it is not our business, that you might want to speak to some of the heaviest users within that 1% and to look at the business case they may present to you.

Q59 Lord Armstrong of Ilminster: If everybody goes fairly fast, might you consider including some of the other authorities in the Bill rather than waiting for subordinate legislation?

Charles Farr: That will be a matter for our Ministers. I cannot anticipate what they would want to do with that.

Lord Armstrong of Ilminster: Speaking personally, I would rather see it in the Bill, if possible.

Q60 David Wright: I think that is a genuine concern, Lord Chairman. People fear that there is mission creep a little on the matters. The more we can get on to the face of the Bill the better it is, because it clarifies the situation. Maybe that is a debate we need to have as we reach our conclusions and report.

Peter Hill: I am sure you know this, but, as you say, there is an order-making power. Any authorities who are not currently on the face of the Bill who would wish to have access extended to them would be contained in an order, which would be subject to affirmative procedure, so there would be a parliamentary vote.

Whether they should be on the face of the Bill is obviously a decision for Ministers. As you say, there is a demonstrative effect. There is also the issue of putting people on the face of the Bill means it is much harder to take them off in future or, if new organisations are formed, there are structural changes, or there are new purposes, it is much harder to make those changes. But, as I say, it is a balance.

Q61 The Chairman: Some of us, who have been around a long time, heard almost those exact words while serving on the RIPA Committee in 2000, where we were dealing with the big four on the face of the Bill and then the Minister, I think, let slip that there were some other public authorities who could be added as well. Under questioning, he then produced a letter to the whole Committee showing that when the Bill was completed there were about 32 public authorities added. Twelve months later, we ended with 500 added and now we have 650. So I wonder: was I lied to then, or are we being conned now?

Peter Hill: I think you have a very clear list of those who might seek access, which is in the existing consolidated order approved by Parliament in 2010. So I think if, collectively, you and we wish to interrogate from a zero base who should have that access, we have the list of the people who we think will want to have that access, and that is the baseline from which to go.

Charles Farr: If I may add, of the 1% of requests that we are talking about—5,000 requests plus or minus—I do come back to the point that the main users are the FSA and local authorities. The rest is a fractional number of requests, somewhere around 500. So I think the FSA and local authorities are the key to this. I honestly do not believe that we are surreptitiously trying to insert major users at the last minute.

The Chairman: No, but Parliament must be concerned with the half of the 1% and the civil liberties of those people.

Charles Farr: I understand.

Q62 The Chairman: Would you accept, to a certain extent, that including some of these more intriguing, lower-level cases, some of the more trivial cases, diminishes to a certain extent the importance of having powers for terrorism, serious crime, paedophilia—the big stuff?

Charles Farr: I do not know whether the offences under investigation by the Financial Services Authority now, of all times, would be regarded as trivial by comparison.

The Chairman: No, but some of the other public authorities of the 650: the Egg Inspectorate?

Charles Farr: I think in the case of some of those—I am not aware of the Egg Inspectorate—their usage is barely in double figures.

The Chairman: So why should they have the power at all?

Charles Farr: Because the double-figure requests that they do make can be very important. If you are investigating an air accident, for example, it is very low usage, but very high dividend.

Q63 Baroness Cohen of Pimlico: There is a perfectly good statutory instrument here, which, if we are going to have a new Bill, I would stick in the back of the Bill—a scheduled plonk. Are we planning to do that?

Peter Hill: Which statutory instrument are you referring to?

Baroness Cohen of Pimlico: Investigatory powers. It has a list of organisations, a very fine list.

Peter Hill: That is the starting point from where people might apply and a version of that, if one went with the order-making route, would then be attached to this Bill. I think, as has been said by the Committee, Ministers wanted to take a zero-based approach and not assume that it was going to be agreed that all those who currently have access through the 2010 order would go on and have that access.

Q64 Lord Jones: Who has real oversight over the current use of communications data and the use that will be made under this draft Bill? We are asking you: who is able to

assure the public and provide evidence to Parliament that the safeguards are proving effective?

Charles Farr: I sense two questions in there. One is an oversight question and one is a safeguards question. If I can perhaps just address the oversight question and you will tell us how much you would like us to talk about the safeguards question.

Lord Jones: You are adept; make your choice.

Charles Farr: Okay, perhaps we can deal with them in that sequence. On the first, oversight of the process, as you know, it is the duty of the Interception Commissioner to keep under review the performance of the duties placed on communications service provides under this Bill—for example, the duty to generate or collect communications data. The Commissioner also provides independent oversight, with his team, of the acquisition of communications data by public authorities and the role of the commissioner will be extended to oversee the new powers, in particular, the collection of further data by industry—CSPs. That will include oversight of testing, regular auditing and inspections.

The Information Commissioner also has a role, particularly on the retention of the data by industry. An Investigatory Powers Tribunal made up of senior judicial figures, which exists already to handle complaints against the intelligence and security authorities, will be extended to cover the provisions here, ensuring that people have an avenue of complaint, should they need it, and independent investigation if they believe the powers have been used unlawfully against them.

The commissioners report to Parliament each year on the use of these powers and their own authorities will be updated to reflect the nature of the capabilities set out in this legislation. That, for me and for us, is the first key way in which oversight of this process is provided to Parliament.

Shall we talk about safeguards? Can I hand over to Peter on that?

Peter Hill: We can obviously give you more information in writing. I am not sure how much you want me to go into, but I would just set out that if you break down the process of the acquisition, the retention, authorisation, and oversight, there are safeguards at each point of the process.

In relation to retention, you will have the order agreed by Parliament following statutory consultation with those affected. You will have the notices detailing what data is to be retained, following discussion with CSPs, and approved by Ministers. You will have all that data destroyed after 12 months. At the storage level, you have that, subject to explicit requirements in the Bill placing obligations on the companies as to the standards for storage. That is overseen by the Information Commissioner. We have talked quite a lot about access, where there is and there will be an approved list of authorities, the purposes for which and the data that they can acquire will be agreed by Parliament and set out in our legislation.

You then have the authorisation process, which is, within those approved bodies, how you get the data, and I think Charles has talked about that. It is the number of people involved in the authorisation process, the considerations that have to be taken into account, the role of the senior responsible owner for the process, and the inspection and auditing of that by the Interception of Communications Commissioner. Of course, a lot of this data will end up in court as part of a criminal prosecution, where it will be subject to the normal rules of disclosure and challenge by defence. There is a filter provided for in the legislation, to try to minimise the data that is disclosed to public authorities to that which is necessary.

There is then, of course, the oversight regimes we have talked about. There is an appeals process, the Investigatory Powers Tribunal. If all that fails, there is a range of penalties set out in existing legislation, whether that is data protection, computer misuse, or misconduct in a public office.

That is a slightly long answer, but I think it is important if you are looking at safeguards, which I am sure you will be, to try to break down the process to what are the safeguards at each stage of that process.

Q65 Lord Jones: It was not over-long, Mr Hill. We need to know just how much you and your colleagues care about oversight and about safeguarding and if you were to write further, you would have the perfect opportunity to put it down. But it is our duty, as parliamentarians, to look at oversight and safeguards. After all, at the end of the day, as Mr Farr said in his previous meeting with us, it is quite simple: it is about liberty; above all else, it is about liberty. Our duty is to ask you these questions and gain from you the kind of informative answer that you have just given to me.

If I may go on, on behalf of the Committee, Parliament is going to be asked to pass the Bill without knowing exactly what data is likely to be sought, the technology that will be used to collect it or how it is used in practice. That is how it comes across to us at this stage; we have not had many sessions of evidence-taking. Public authorities will be added by order and the permitted purposes can be varied by order. What is exercising our minds at this moment on these matters, which you have responded to, is whether Parliament will really have any oversight powers.

Charles Farr: If I may, you raise a question about the degree to which you are given information about what exactly this legislation is going to lead to. I would emphasise, as we did in answer to a previous question, that the definition of "communications data" is clearly set out in existing legislation and there is no change to that here. So I would reassure you that there is nothing in this legislation that is going to amend existing definitions of what communications data is. We continue to think of it, as we have done before, in three categories: subscriber data, service usage data, and traffic data. We are happy to send you further details about what exactly those mean, but that will provide the essential context for any order made under this legislation, and there is no intention to change data definitions at all.

Q66 Lord Strasburger: You might have picked up that certain Members of the Committee are concerned about a certain looseness in the drafting of the this draft Bill, and I pick up another one. Clause 4(2) seems to make it possible for data to be retained not just for 12 months but indefinitely; all a public authority has to do is to notify the telecommunications operator concerned that the data is or may be required for the purpose of legal proceedings. So there seems to be quite a big loophole there for a public authority to extend the retention of data indefinitely, just on the basis that it asserts that it might be required for legal proceedings.

Charles Farr: As you know, communications data is evidentiary. It is used as evidence in court and it is essential that the Bill facilitates that process in the future, as it has in the past. That means that data has to be retained until the court procedure takes place, so I see no alternative to having a clause of that kind. If the clause needs to be more tightly drawn, or if there needs to be greater clarity about the evidence or the material that needs to be put forward to support that application, to demonstrate that criminal proceedings are, indeed, in the offing or planned and that the data is, indeed, intended as evidence, we can take that away and look at that.

Lord Strasburger: I think what I am saying is that my colleagues on the Committee have drawn to your attention various items, like this one, where there is a lot of opportunity for mission creep. I just draw this one to your attention as yet another example of it.

Q67 Dr Huppert: My apologies again for having to present my Bill—successfully on this occasion.

Mr Farr, if I can start off just by talking about the retention period for data, the EU data retention directive gives flexibility, as I understand it, to keep data for between six months and 24 months. Why have you gone for 12 months in this? What was the evidence for that?

Charles Farr: Obviously, we consulted the major users quite widely on this issue and we have also looked at, and have more recent evidence about, the types of data, the purposes for which it is obtained—we have talked to the Committee about that—and, in particular, the period of time for which the data has been retained by the time we seek access to it. We have also correlated those variables together. So we are able to determine, for example, that, as a matter of interest, claims for communications data in connection with terrorism tend to refer to data which has been stored between six months and 12 months, whereas applications for data in connection with certain other crime types, generally speaking, are for data which has been retained for rather less.

So we consulted and we have looked at the data. We can provide you with the data that is relevant to the latest survey that we have done. In summary, we are satisfied that data retention for a year is required across the range of crime types in connection with which data is applied for, and there is a significant amount of data at the outer end of that period, i.e. between six months and a year, for which the police need access.

Q68 Dr Huppert: I hope you will be able to share all of that data with the Committee and the wider public. Can you give me a sense: of the 552,550 data requests in 2010, how much was, say, less than a month old? Was any of it more than a year old?

Peter Hill: Was that in relation to 2010?

***Charles Farr*:** Yes.

Peter Hill: In relation to 2010—

Dr Huppert: I will take 2009 if you have it.

Peter Hill: Let us take the data that we think we will have towards the end of this month. The data for 2010, around 30% of that was accessed between six and 12 months.

Dr Huppert: Are you saying you do not have the full year's data?

Peter Hill: The data on the age of data is based on the snapshot surveys. It is not reported in the Interception of Communications Commissioner's report.

Q69 Dr Huppert: Perhaps I am misreading the Data Retention (EC Directive) Regulations 2009, 9(2)(b), which says that the public communications provider must provide the time between data being retained and requested for every single incident. You must collect that data.

Peter Hill: We return that data to the Commission and the last return we made was for 2010. So the last return that we made to the Commission relates to—so the last data that we have, in addition to the data I was about to give you, related to 2010.

Q70 Dr Huppert: So for 2010 you have full figures for all of those 550,000.

Peter Hill: Yes.

Dr Huppert: And you could share with the Committee the age profile for all of that.

Peter Hill: So we can share with you the age profile for what we know about the 2010 data and, in relation to the 2010 data, around 30% of that was for data between six and 12 months—sorry, for more than six months.

Dr Huppert: So some of it was more than 12 months.

Peter Hill: Yes. So, we cannot require the retention of data after 12 months, but, for example, in relation to subscriber data, businesses may need that for their own business purposes. So 70% was for up to six months and six and beyond was 30%.

Q71 Dr Huppert: If you have all the data, I think it would be very useful to have the breakdowns in number of units. It seems to me that a lot of it would be, in many cases, data within the last week for a missing person investigation.

Charles Farr: Just to be absolutely clear, in the case of terrorist inquiries, there was a significant amount of data required, which has been stored for significantly longer than a week and, generally speaking, between six months and a year. A criminal investigation, particularly an investigation in terrorism, would be very seriously hampered by the reduction of data retention periods to a period of a week or more.

Q72 Dr Huppert: Mr Hill says he has the data to back that up, so I hope you will be able to send it to us and we will be able to look at it for ourselves.

Peter Hill: Yes. The more serious crimes and the more complex crimes generally access data in that later period more than with more simple crimes.

Q73 Dr Huppert: I look forward to seeing the data. Can I then move us on to the other issue—I do not want to take too much time, having missed so much—about costs? The Home Office estimate is that the cost of this Bill as it currently is would be £1.8 billion over the next 10 years. It seems to be very unclear what is included within that cost, partly because it is not yet clear whether you would be able to obtain data by negotiation or whether it would require significant infrastructure, DPI techniques and so forth. What does that £1.8 billion cover?

Charles Farr: We have talked about DPI and when DPI might be used and the circumstances in which it would be used, and I emphasised, of course, that DPI is not central to this legislation. So the likely areas of expenditure are as follows: (a) new systems to enable CSPs to store and process data, including not only telephony but internet-related data too; (b) an improved infrastructure enabling acquisition of data as it transits the UK, where necessary; (c) business change and training in law enforcement agencies to make use of new data in criminal investigations; (d) some horizon scanning and experimentation, and I would emphasise that is a small amount, to understand continued technical change and future stakeholder requirements to manage risk; and (e) the setting up of a body to sustain the capabilities of the CCD comms data programme after our build programme has terminated.

Q74 Dr Huppert: So if it turned out that you could not get the agreements you wanted and you need to do more DPI-type data collection, the costs would go up significantly from this £1.8 billion, presumably.

Charles Farr: No, I think—

Dr Huppert: So the £1.8 billion assumes doing a lot of DPI.

Charles Farr: The £1.8 billion assumes doing a certain amount of DPI, but not that DPI is central to this proposal.

Richard Alcock: The majority of the costs are around data retention. Over 50% of the costs are associated with working with communications service providers in the UK and overseas, to establish data retention stores, build on the very good practice that we have at the present time and put in place the infrastructure to secure the access of that information from law enforcement. The costings reflect our strategy, which is that we will spend more on data retention, and that, indeed, is what the focus of the programme is.

Q75 Dr Huppert: Just so that I am clear, an overseas-based company that agreed to store this data for you—Google, Facebook, whoever it may be—you would pay the costs that they tell you they have for doing that; is that right?

Richard Alcock: Not that they tell us. We would work with the communications provider to establish what we needed them to collect in addition to that which may already be retained. What we would be seeking to do is just pay the difference between that which they currently are or may be retaining and that which we may want them to retain.

Dr Huppert: I suspect they will have an interest in trying to inflate that cost, but you will fundamentally be paying overseas companies.

Richard Alcock: It would be audited.

Q76 Dr Huppert: Can I then turn to the flipside—I am rushing through this somewhat; I apologise—which is the benefits? There is a section in the information that was provided that had very little information about benefits and came up with a figure of up to £6 billion, I think it was, over 10 years. Where does that figure of £6 billion come from, and can you evidence it?

Charles Farr: The answer to both of those questions is it comes from us, validated by the Treasury and our own economists. How do we validate it? If I can briefly take you through the methodology, you can make your own judgment.

The benefits assessment was taken from a sample of 13 stakeholders across the user community, including those stakeholders making the most use of communications data. We began with a survey for them of the likely trajectory of communications and communications industry, informed by our own work and, indeed, by Ofcom. We then asked them for an estimate of how communications data was helping the resolution of crime and the protection of vulnerable people now, and their view about how it was likely to do so in the future. We then attached a monetary value to lives saved and obviously an estimate of revenue recovered. The monetary value for lives saved was based on an existing calculation in that regard made by Home Office economists, used for wider purposes in crime work. We can give you the reference of the relevant documentation and, indeed, provide you with copies of it, but it does attach an economic value. We then made the required calculation. I should emphasise that that net benefit is the benefit deriving from those 13 stakeholders only, not a nationwide survey of all users of communications data. Moreover, the financial value of the benefit does not take account of any financial value that you could put on a murder, because we could not find a sensible, credible, decent way of doing that, nor on a terrorist incident.

In our judgment, the methodology is sound. It was endorsed by Home Office economists. It went to the Treasury. It was in line with Treasury guidance on investment appraisal but, in fact, it does not capture the totality of benefits, because it was based on a survey of 13 organisations and it does not monetise some key benefits for which monetary value was hard to attach.

Q77 Dr Huppert: While prediction is always hard to do, and I totally accept that all of these things are, to some extent, estimates, presumably, given that you currently have 75% of the data that you would want and you are trying to go up to, let us say, 90%, because it will not be 100%—

Richard Alcock: We said 85% earlier.

Dr Huppert: 85%, fine, so that makes the case even easier. Then you are saying there should be benefits of £600 million a year times 7.5 that you can already evidence for the last year. So, presumably, you would be able to supply this Committee with an estimate of the calculation that shows whatever that comes to, £4 billion a year or so, in the last year that was saved or the net benefit as a result of the communications data that we had access to.

Richard Alcock: The benefits calculation is about, essentially, trying to quantify, in monetary terms, that which could be accrued should the Bill be passed.

Dr Huppert: My point is that the communications data you already have, you will know the benefits we accrued last year from that and, presumably, if your methodology works, you should be able to point to where some of that lies.

Richard Alcock: That presupposes we have all the data that is required. We will take that away and have a look at it.

Q78 Dr Huppert: I think that would be helpful. One last question, if I may, Lord Chairman; sorry to presume on this. A lot of the costings and the work rely on this close relationship with the CSPs. I apologise if this has already been asked, but you, presumably, have been working quite closely with the major CSPs; I will not ask for a list of everybody you have spoken to, but I expect we can guess who the major ones would be. In your view, are they all happy with the Bill as it currently is?

Charles Farr: We have referred to that earlier, but perhaps I may repeat what we said. You are right, of course. As you well know, we work not with every CSP but with the major CSPs who are of primary concern to us. We have a good, collaborative and, I believe, constructive relationship with those CSPs, who, I believe, recognise that they have legal obligations and other obligations to provide data in certain circumstances: where it saves lives and helps us convict criminals and protect innocent people. They also completely understand that a gap is emerging between the data that they have and the data that we require. They are saying to us, very clearly, in terms, that they would expect legislation to provide a means for narrowing that gap and that if the legislation so provides, they will work with us to help us to do that.

Q79 Dr Huppert: So if we asked them the direct question "Are you happy with this Bill?" when a range of these people come before us—

Charles Farr: I cannot tell you whether they are happy with it. I can tell you what they tell us—and I emphasise I am not talking about every CSP; you can doubtless find one that will have a problem with this—which is that the major CSPs understand the problem that we are trying to solve, understand the technology and the way in which we are proposing to solve it, agree that that technology is feasible and are looking for legislation to underpin collaboration in the future. Whether that means happy or not, I hesitate to say.

Q80 The Chairman: Before I ask some other colleagues to participate, could I stress that the Committee would like, then, to get a paper on the historical data of how many lives saved, children safeguarded and money recovered, which would help us come to a conclusion on whether the extrapolated data or the plans for the next 10 years are optimistic or not. And I think we would like the figures from your economist on what is your standard estimate for a life saved or a child safeguarded.

Charles Farr: If I may, the second request, of course, is well understood and we can provide the paper, which was done by the Home Office economist. On the first, we had a similar conversation before. Acquiring that data retrospectively is not straightforward and we will have to look and see what we can do, talking to all the stakeholders about the evidence for that in the past as well as the evidence going forward.

The Chairman: I presume we may put this to HMRC when we see them and we will have the HMRC—

Charles Farr: In some ways, the figures for HMRC are easier to come by, because the financial benefits are easily understandable.

Q81 Michael Ellis: Mr Farr, as far as the impact that would follow should the period for which the data should be retained be reduced, could you say something about the effect of that if the Bill was to be altered to reduce it from 12 months?

Charles Farr: I know that you will want to discuss that with the police, so, if I may, because it is more central to our role and my own background, let me say that removing, if one chose to do so, a retention period of a year and reducing that to, say, less than six months would have a significant and serious impact on our ability to investigate terrorism. That is true for terrorism, in particular, because it is often long in the planning and one has to go back to the beginning of the plot to understand, with certainty, who has been involved with it at every step of the way, not only in this country, but overseas as well, because remember, data shows us international connections as well as domestic ones.

Michael Ellis: So you would consider a period of less than 12 months to be untenable as far as the investigation of terrorist offences is concerned.

Charles Farr: Obviously, you will talk to the police and the IC may talk to the agencies. I think it would be very challenging for the investigation of certain crimes, in particular terrorism.

Q82 Stephen Mosley: Clause 1 gives the Secretary of State strong powers in order to specify which communications service providers need to keep the data and, also, to specify what technology they should use. I know that most of them are broadly happy, but what happens if you specify something and the service provider says, "No, there is a better way of doing it"? Is there any sort of right of appeal or is it a general situation that you would negotiate on an individual basis? Are you looking at standardised technology?

Moving on a bit from that, without asking for specifics, because I can fully understand why you would not want to give specifics, have you got any idea of the general number of CSPs you would be looking at? Are you just looking at public network providers or will you also be looking at private networks, which of course moves us on to the big issue of last summer, which is BlackBerry Messenger? Will that be included?

Charles Far: On your two questions, let me have a go at the first and then perhaps Richard or Peter can talk more competently than me on the second. I emphasise that it is exactly the purpose of this legislation to facilitate a dialogue with industry about the best way to address some of the problems that we have. I have no doubt that some CSPs will have much better ideas about how to address these problems than will we and our technical colleagues and others, and there must be a conversation. I believe firmly that the groups and the relationships we have set up over the past few years to deal with all manner of issues to do with data and interception will facilitate that process and provide for it.

On the second issue, if I may, I will turn to Richard.

Richard Alcock: In terms of the general number of CSPs, just in the United Kingdom, I think it is in the order of 250 to 300 communications service providers. We certainly do not envisage working with that many within the piece. Clearly, it depends how communications services change over time and whether groups gravitate to a certain service or not. But we certainly do not envisage working with everyone, and I estimate it will be a relatively small proportion of those.

Peter Hill: It may just be worth mentioning that although we do not envisage getting into dispute or confrontation with any CSP about the notice that we would serve on them, there is, as you probably know, an arbitration body, which was set up to deal with interception and is, under this legislation, going to have its remit extended to communications data. That brings together the industry and the public authorities to arbitrate a disagreement over a particular notice and then to make recommendations to the Secretary of State about whether

that notice should be maintained, modified or removed. So there is an ultimate route of mutually consensual arbitration.

Q83 Stephen Mosley: In terms of private networks, we are thinking in terms of the internet here: internal private company networks, the internal government network, and BlackBerry Messenger. Would they be included?

Richard Alcock: We cannot talk about individual providers, but the Bill does enable notices to be served on both public and private networks.

Q84 Mr Brown: Can I ask about the use of warrants rather than the use of a more senior official to give consents for data searches? Where local authorities are seeking data they are being asked to go and see the magistrate. Why did you do it one way for local authorities but have a different route for the internal workings of the state?

Charles Farr: The Government, at the time of the protection of freedoms legislation, took the view that confidence in the authorisation process for seeking access to communications data within a local authority had been damaged by events which you will be very well aware of and which have been subject to media reporting, and that that authorisation process should be changed and that, therefore, a magistrate's approval was appropriate. Similar concerns had not been expressed about the authorisation process in the police and had not emerged in quite the same way in the Interception of Communications Commissioner's report on these matters. Moreover, there is a practical, significant problem that local authority requests for communications data constitute about 0.3% of the whole; police requests constitute, with the security services, 99%. So there is a volume, practicality and logistics aspect involved in moving the bulk of communications data requests across to the magistrates' warrant system.

Q85 Mr Brown: I appreciate the practical point, but can I put two what seem to me possible snags to you? When searching for an appropriate magistrate, people always seem to find the one who will give them the answer they want rather than the one who might take a more robust and independent view. How strong a safeguard is that? Secondly, where the senior officer may be working day to day with a more junior officer, giving the authorisation, is there not a danger that there will be familiarity and a canteen culture and that people will give the approval too easily?

Charles Farr: On the first point, I recognise the potential problem. Of course, we are only beginning to roll out magistrates' authorisation for local authority requests and I think we probably have to see how it goes and then come to a judgment. I am sure the Interception of Communications Commissioner will come to a judgment on that as well.

Q86 Mr Brown: That does not really make it a very robust safeguard. What is the magistrate's function?

Charles Farr: I think my point is it remains to be seen. It is a response to concerns which have been expressed about internal authorisations and the specific environment of local authorities and incidents that had taken place connected to applications for communications data. I think a magistrate will impose greater discipline on that process. The Government has not seen the need to do that for other public authorities. We will have to see, I think in the commissioner's report, how effective it is going to be with local authorities. It is too early to say yet; the process has not begun.

If I may, I will ask Peter to comment on your second question, which is whether, as I see it, a sort of informal network in other public authorities may facilitate, in an unhealthy way, applications for communications data.

Q87 Mr Brown: We are all human. Where is the safeguard?

Peter Hill: It lies in the authorisation process. So, firstly, I think sometimes there is an idea that there is a police officer sitting at a computer terminal who can access communications data when they like. That is not how the system works. There are a small number across the country of accredited, trained, identified single point of contacts. By "identified", I mean they have a unique PIN number which allows them access to the system, so it is not the question that anyone can log on and pull off this data.

The person authorising it at the senior level should be unconnected to the investigation. So there will be an investigator saying, "I think communications data might be useful in this process". They will go to the specialist and say, "What sort of data might I be able to get?" Together, they will come up with an application. The senior officer will then say, "Do I agree that it is necessary and proportionate?" and then the specialist, the single point of contact, will issue the authorisation, log on to the system and get the data, so there are a number of people involved in that process, overseen by a senior responsible owner in the police authority. Of course, that process produces the audit logs. Those are inspected by the Interception of Communications Commissioner. He reports on the use that the police and everyone else makes of those powers. In the end, many of these cases end up in court, so the communications data will then be subject to the normal processes.

It is a rather long answer, I am afraid, but it is useful, I think, to know what the internal authorisation process is within the police to understand that it is not simply a question of somebody sitting at their desk, their mate next door asking for some data, and them logging on and pulling it off.

Q88 Mr Brown: I think it is helpful to us to have that explained in the way that you just have done.

Charles Farr: I just wanted to reinforce the point—and I apologise for the obscure language—about the single point of contact inside the police, who, as Peter has said, is there both to offer technical advice to the applicant—the person running the investigation who thinks they need communications data—and to facilitate access when approval is granted. The special point of contact is someone whom we are responsible for providing training programmes for and whose training and security we take extremely seriously, as, indeed, do the police. It is not a casual appointment and a casual part of someone's career in the police. I hope, when you talk to the police, that you are able to get from them a sense of what the SPOC, so-called, means and does, and that will reassure you about the thoroughness with which that role is approached by people who are in it.

Q89 Mr Brown: Has any information that you have obtained so far been improperly released by people who should not have released it, and have they been caught and prosecuted for so doing?

Charles Farr: The Interception of Communications Commissioner's report is due out on Friday. I hesitate to pre-empt what he may say on this, but of course it is part of his job to look at instances where the system has not behaved in a way that it is intended to do.

Q90 Mr Brown: On the prosecution point, how often was the offence of misconduct in public office prosecuted last year?

Charles Farr: In general?

Mr Brown: It is almost always about a public official obtaining information and selling it on, usually, but not always, to a newspaper, maybe working through a private detective and then using it, usually, for selling newspapers.

Charles Farr: Peter may have the statistics, but, as you know, there are a number of investigations under way at present, which are adjacent to this.

Q91 Mr Brown: You can see why this would be at the forefront of the public's mind.

Charles Farr: I can understand that, yes.

Peter Hill: All I can say is that in the reports that I am sure you will have seen, and you will see when the latest report is issued in the next few days, there have been, so far, no occasions when Sir Paul Kennedy, the inspector, has identified what one might call wilful or reckless errors or releases of data. Of course, as in any system, there are errors, but what I think you are talking about is either something that is wilful, reckless or criminal and, so far, the inspection regime in relation to communications data—and I hasten to add that this is in relations to communications data—has not identified such cases.

Q92 Mr Brown: If caught, what would you say to me to convince me that somebody who had done such a thing would be robustly punished? Under what offence would they be prosecuted?

Peter Hill: There are, as I am sure you know, a number of offences on the statute book. Under the Computer Misuse Act, it is possible to prosecute people; there are custodial offences there, for a number of years. If it is a data protection offence, there are the offences in the Data Protection Act.

Charles Farr: Currently under review, of course, in relation to Section 55.

Peter Hill: Yes, and of course there are the misconduct in a public office offences, which carry, potentially, extremely serious custodial sentences.

Q93 The Chairman: There is nothing on the face of this Bill to reassure the public that any abuse of power from a police officer or any other officer or designated person will be treated very seriously. Why not put some criminal sanctions in the Bill?

Peter Hill: We can certainly take that away.

The Chairman: We look forward to Sir Paul's latest report. It just seemed to me, reading the 2010 one, where 94% were performing satisfactorily or were good, one wonders what the other 6% were like, or that 44 police forces were up to speed, but two were very poor in the way they treated data. It just seems to me that the sanctions in those cases were about a bit more training and a bit more advice, whereas if there was the possibility of a criminal penalty there, whether or not it was used, it might reassure the public. I am sorry, Mr Brown.

Mr Brown: I happy to leave it there for now, but I think we should return to this and there is a doubt in my mind as to whether the criminal sanctions work.

The Chairman: If you have any further advice to give us on criminal sanctions, we will happily receive a paper on it, but we will wish to return to this, as Mr Brown said.

Q94 Stephen Mosley: There is one big difference with this Bill: Clauses 14 to 16 establish a request filter, which seems to me to be an incredibly powerful tool. It will allow the people who are accessing the data to basically scan all of these individual databases and bring the results into one place; it will be a very powerful tool. It will be operated, as I understand, it says, by the Home Office. What sort of checks and balances will be on this new tool? How will it work?

Charles Farr: The Interception of Communications Commissioner's powers are, of course, being extended with specific reference to the request filter. There will be very detailed audit logs indicating exactly what requests have been made, what results have been produced and, of course, an examination and confirmation of the fact that extraneous data has been

destroyed and never makes it to the public authority in what is an automated process. So there is quite a lot of reassurance built around new oversight bodies plus new automation plus new audit controls.

On ownership, I think Ministers certainly envisage that a tool of this kind must be operated by a public authority. It is possible that, as the NCA builds, that might provide a home for a capability of this kind, but I think until such time as it has, it is premature to make a clear conclusion beyond saying, of course, that a public authority will own and operate this—at present, the Home Office.

Peter Hill: I think you used the word "databases". Just to be clear, the filter only relates to accessing communications data. So a request will be made, for example, to know who the subscriber to an e-mail was, or "This phone was in these locations", and it will take that communications data. First of all, it will tell the person asking how much data is likely to be necessary to answer that query, so it will help them make the judgment about necessity and proportionality. If they go ahead, it will then sift out the irrelevant data and give them the relevant data, not the data they do not need. I entirely take the point that it is a tool that can do a lot of things, but the point that this is a safeguard to try to focus the data that is being asked for is an important one. Rather than getting all the data and then sorting it within a police authority in order to get the bits you need, having a process which does that without human involvement should reduce the data that is being disclosed, not increase it.

Stephen Mosley: So, effectively, it will interrogate the communications data that is held by the third parties and bring the results to one place.

Richard Alcock: Yes, on a request-by-request basis.

Q95 Lord Armstrong of Ilminster: I think the legislation says that things would be authorised by senior designated officers, and that those officers would be defined in negative orders before Parliament. I think there are two things on this. First of all, I believe that in the police the usual rank is superintendent, and I wonder whether superintendents are not a bit too close to the coalface and the operation, and therefore whether it should not be a chief officer who is required to give authorisation.

Secondly, is it is good enough for the senior designated officer to be labelled by a negative order? Should Parliament have slightly more say in how that is applied, not just in the police but in other services or authorities?

Charles Farr: Perhaps I can take the first of those two questions and Peter can deal with the second, on the negative order. I think there is, as you have realised and seen, a set of serious issues around the appropriate level for a senior designated officer. The police will doubtless comment on this, if you ask them. I think there obviously is a case for pushing up that level to a senior ACPO-level person. We looked at that, and Ministers were persuaded that that was not necessarily appropriate, because a superintendent perhaps has a closer feel for the day-to-day operations and, therefore, has a better sense of necessity and proportionality, probably has more time to devote to a particular application and, critically, of course, is still separate from the investigation. As in Peter's answer to the earlier question, they must not be a part of that investigation and can remain detached for it. For all those reasons, Ministers were persuaded that a superintendent remained the right level, rather than pushing it up to an ACC or a DCC at ACPO level. However, there are clearly alternative views and you will, I am sure, ask the police about that.

Can we address the second issue?

Peter Hill: On the second, I need to go back and check, but my understanding is that the order that sets the authorities, the purposes and the approvals levels is by affirmative procedure, not negative. We can come back to you and confirm that.

Lord Armstrong of Ilminster: If that is right, that deals with that question.

Charles Farr: We will check that.

Q96 The Chairman: Finally, Mr Farr, I think you have said that the driving force behind this Bill was voluntary collaboration and co-operation with the CSPs. You have had informal assurances or verbal assurances from them. Have you had anything in writing from chief executive officers of some of the big CSPs that they will play ball?

Charles Farr: Richard may be able to correct me, but we have not sought anything. I do not think we would intend to do so. That would look, I think, less than collaborative. Our Ministers have talked to senior office holders in those companies, and I think we have received the assurances that we would expect.

The Chairman: "My word is my bond", yes.

Baroness Cohen of Pimlico: You do not need civility if you have legislation.

The Chairman: Thank you very much, gentlemen. It has been a long session, but this was a very important opening session. It has been much longer than I expected, but we are determined, in this Committee, to be very thorough in every session. By the time we report we hope we will have looked at absolutely every aspect of the Bill and the proposed legislation. Thank you all very much.