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

HOUSE OF LORDS

HOUSE OF COMMONS

ORAL EVIDENCE

TAKEN BEFORE THE

JOINT COMMITTEE ON THE DRAFT COMMUNICATIONS DATA BILL

THE DRAFT COMMUNICATIONS DATA BILL

TUESDAY 30 OCTOBER 2012

TREFOR DAVIES, DAVID WALKER, CASPAR BOWDEN AND DR GUS HOSEIN

STEVE HIGGINS, SIR PETER FAHY, PETER DAVIES, ALAN LYON AND DAVID STEVENSON

Evidence heard in Public Questions 1013 - 1140

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.

Oral Evidence

Taken before the Joint Committee on the Draft Communications Data Bill

on Tuesday 30 October 2012

Members present:

Lord Blencathra (Chair)
Lord Armstrong of Ilminster
Baroness Cohen of Pimlico
Lord Faulks
Lord Jones
Lord Strasburger
Nick Brown
Michael Ellis
Dr Julian Huppert
Stephen Mosley
Craig Whittaker

Examination of Witnesses

Witnesses: **Trefor Davies**, Chief Technology Officer, Timico Ltd, **David Walker**, Managing Director, Labelled Security Ltd, **Caspar Bowden**, Independent Privacy Advocate, and **Dr Gus Hosein**, Executive Director, Privacy International, examined.

Q1013 The Chairman: A very warm welcome to you, gentlemen. Dr Hosein, welcome back for the second time. For the benefit of the public record, we were trying to question Dr Hosein a few weeks ago and we were interrupted by so many votes he did not get much of a chance to give evidence. Just for the record as well, perhaps if you would all state who you are.

Trefor Davies: My name is Trefor Davies. I am the CTO of an ISP called Timico.

Dr Hosein: My name is Gus Hosein and I am the Executive Director of Privacy International.

David Walker: Dave Walker, Managing Director, Labelled Security Limited, but just here representing myself.

Caspar Bowden: Caspar Bowden. I am an independent privacy advocate. Formerly, I was Director of FIPR and, more recently, Chief Privacy Adviser to Microsoft, but I represent nobody other than myself at this meeting.

The Chairman: Thank you very much. We are very grateful to you for coming and we are looking forward to the evidence you have to give us.

Q1014 Dr Huppert: It is very good to see the four of you here. One of the issues that I think a number of you have raised concerns about is how broad Clause 1 of the draft Bill is. It captures a huge range of information. This is related to the Home Office's claimed data gap. Last week, we were told in public session by the Home Office that their intention was to use the Bill to plug two specific areas of the data gap: information relating to IP addresses, and information relating to weblogs. If the legislation could be drafted narrowly to only allow notices to capture those areas from CSPs domestically, would that significantly allay your fears about the scope of the draft Bill?

Trefor Davies: I take it from when you say "weblogs", you mean details of websites visited.

Q1015 Dr Huppert: Only up to the first slash, as is currently allowed under RIPA, without the identifying features later, but which is not kept currently if it is not for business purposes.

Trefor Davies: There are two sides to this discussion. One is the straight technical side from an ISP's perspective. Many ISPs will already store information of the IP addresses. As a business ISP, we only provide people with fixed IP addresses, and these will not change from one year to the next, to be honest. The bigger consumer guys and the mobile ones may well change them quite often and so, physically, it is probably not too difficult a thing to do.

From the weblog information, most small ISPs would probably have to put some investment in technology in order to be able to support it, but again it is not too difficult a thing to get your brain around.

I guess from the point of view of the other side, which is the privacy side, it is whether narrowing down the information to just those two areas significantly reduces the amount of information that you can drill into about a person. We saw some responses in the written responses; one was from the Tor Project, who said that, "23.3% of Wikipedia users could be uniquely identified from the 'use data'". You only have to look at the recent news that came out about the Houses of Parliament, that there are only two IP addresses that are used to access the internet from here and that it was possible to see that a number of the Members' Wikipedia profiles had been modified from within the Houses of Parliament. Therefore, you could say that a lot of information could be gleaned about somebody still if you were drilling into or fishing IP address information.

Q1016 The Chairman: Members of the panel, if you have something to say, say it. It is not just one each, but if you have nothing else to add then we will move on.

Dr Hosein: Following this revelation last week, we did a consultation with our friends and colleagues in industry, both domestic and abroad. When we spoke with the telecommunications companies domestically, they informed us that already do record the information the Home Office is seeking under the Digital Economy Act, so would not require any of this discussion. This Bill is not necessary for achieving that objective.

Talking about weblogs of, say, the providers, the foreign service providers, for instance, when we spoke with some of the major players, whose names I cannot mention, they expressed their concern about the idea of being compelled to collect this information. Although they process it, they do not collect it and they do not store it, and this entire scenario seems to be generated because we are still using IP version 4 and they believe this will all be solved within a couple of years when everybody moves to IP version 6. So it does seem odd that we have this massive piece of legislation with a vague objective to solve such a small problem that, in a sense, is solvable already domestically.

Q1017 Dr Huppert: Can I just bring you back to the Digital Economy Act issue, a controversial piece of legislation, as you know? Are you saying that all of the domestic providers specifically have everything that the Home Office said last week, and would any of these providers, even anonymously, be able to write to this Committee to confirm that? Because I think it would be very helpful if, in fact, they already have it all.

Dr Hosein: Yes. I asked one of the providers for them to say so publicly and they responded saying they already have, in a submission to Ofcom, so in our written evidence the first footnote refers to exactly that public source where they state as much.

Caspar Bowden: I do not know what was said to the Committee in secret session by the Home Office, so I am trying to read between the lines about what information you have received about weblogs and IP addresses. Certainly one aspect of this that I have been concerned with at European level is I have been sitting as an independent expert on the European Committee to implement the data retention directive for the past three years, and this subject has cropped up, as you might expect, in that committee. I will just rehearse and clarify what the issue is here. We are talking, by weblogs, about logs of websites visited retained by the internet service provider and the internet service provider would only be able to do this by, essentially, intercepting the stream of packets en route to that third party website, because, as it were, that traffic between the user's computer and some other website is, in a sense, nothing to do with the internet provider. The internet provider's function is merely to convey packets from A to B.

Q1018 Dr Huppert: But it knows, presumably, where B is in order to convey the packet to B.

Caspar Bowden: Not really, because at that level the packets are just datagrams, which are just passing through the internet service provider's pipes. Sometimes internet providers used to operate something called a "transparent cache" or "transparent proxy" where they would keep copies of frequently requested webpages from all over the internet as a local copy, but that is really not done very much now at all. I think the Committee should be clear that this proposal for ISPs to log websites visited is intrusive and, frankly, it lacks a legal basis. There is no basis for doing this currently, as I understand it, under UK laws or secondary legislation that has currently been enacted, nor is there any legal basis for doing this under the European data retention. Now, there are technicalities in European data retention and the intersection between European and domestic law which might permit this, but it is, I would say, dubious. Indeed, if this is going on today—if internet service providers are retaining website information about websites visited—this is something that was discussed by the European Committee, and European data protection authorities took the view that this was illegal.

Q1019 Dr Huppert: I must say we are getting different messages. Mr Davies says that this is easy to do, Dr Hosein says that it is already legally required, and Mr Bowden says that it cannot be done.

Dr Hosein: I think we are talking about different aspects of it. What I was speaking about was whether or not a domestic mobile phone provider would record the IP address given to a user and the source port that was granted to that user for that moment in time, so that may be recorded by the domestic mobile phone company.

Q1020 Dr Huppert: So not the URLs that they go to up to the first slash.

Dr Hosein: Caspar is addressing the URL issue.

Caspar Bowden: There are two different issues: the website logging issue and then the IP and source port number issue; they are totally different issues.

David Walker: I agree with Dr Hosein that it is a curious matter of timing, in that the nature of proxying that has been required with IPv4, which can be used, has an unfortunate side effect, from the point of view of the Committee here, that it often conceals the location or nature of a user. That issue is going to, effectively, go away in the next couple of years with the adoption of IPv6, which will have them for sound commercial reasons.

In terms of the capturing of URL data up to the first slash, it is a very interesting question regarding whether that capture is feasible from the point of view of whether or not that data is concealed cryptographically at the point at which interception is intended or

possible to occur, rather than what was said about Wikipedia, for instance. Wikipedia, even though it has cleartext access, is able to identify all the URLs because it would be able to terminate any cryptographic connections to it, whereas if all this information is to be gathered purely by the ISPs, they may be looking just at ciphertext, at which point the data will not be recoverable.

Trefor Davies: I would like to add that we would not be able to detect encrypted URL data.

Q1021 The Chairman: We understand there are three categories: open messages where you can get everything—the URL and the content; ones where the content may be encrypted but you can get the URL; and ones where the URL and content is fully encrypted and you cannot capture anything. That is, I think, my understanding.

David Walker: Yes.

Q1022 Dr Huppert: Encryption is something that we recognise is a problem and what you said is very helpful. I am still trying to perhaps pin you down to "yes" or "no" answers, if they are appropriate. If Clause 1 was restricted just to either or both of those specific issues would that, in your view, (a) make the Bill better and (b) make it acceptable?

Dr Hosein: You do not need a Bill, in my view. You do not need this Bill in order to do any of that.

Q1023 Dr Huppert: But a changed Bill.

Dr Hosein: The point I was trying to make was that this data is already collected here, in this country. You could try to pass a piece of legislation requiring foreign providers to record this information, but they are more likely to laugh than to adhere to it.

Q1024 Dr Huppert: So the IP data can be done without the legislation and the weblogging, you say, is very hard to do.

Caspar Bowden: I think it is legally hard and in terms of human rights it is hard, because if I understand your point correctly, it is about whether we take the premise of Clause 1: that there shall be blanket retention for everybody in the country of certain categories of data. That is still extremely problematic in human rights terms, so I would want to refocus the question on whether the fundamental methodology is collecting data about people about which there is reason to collect—whether there is some basis of suspicion, whether they are in vulnerable groups. To take a rough figure, it is about whether we are talking about 1% of the population, as opposed to recording data about 100% of the population. That seems to me the essential principle at stake.

Trefor Davies: I am not sure that it really does reduce the scope that much. Looking at the original proposal, which is fairly unclear because a lot of it is left deliberately unclear, in my mind, a lot of what might be asked of the ISPs to do is very difficult and it comes down to the encryption and the data being held overseas. If you take away that aspect of it, which is very difficult, you are down to relatively straightforward things, but it becomes about privacy and non-technical debates, because I believe that all of this database will eventually find its way to the public domain and people will be having a play with it.

Q1025 Dr Huppert: One of the issues the Home Office has raised is the idea of future-proofing—that the information they need will change in the next few years and a few years after that. There is no doubt technology is changing. Do you accept their argument about the need to future-proof the legislation and what advice would you give us on how to pass legislation practically, if it is required, in this sort of ever-changing world?

Trefor Davies: If you are buying into the concept of storing all the information and trying to catch criminals, then it would be a natural thing to provide future-proofing to it. My only technical observation is that people developing applications and services these days are far more conscious of the need to build privacy into their applications and services. You can think of Apple iMessage. Even Skype, for example, is designed to be a private means of communication. I think that future-proofing it as a sort of blanket open book is not necessarily going to have much benefit, because the technical issues are going to be there.

Dr Hosein: If I put my academic hat on for a second, there is no such thing as future-proofing. An attempt to make something technology-neutral is a political act. It is an attempt to say that our understanding now is all we will ever understand, regardless of how the environment changes over a period of time. In the first question you heard the answer about IPv4 versus IPv6. That is going to change in two years, so why are we talking about a program over a 10-year period? If we look at, say, the debate we had 12 years ago about RIPA when we were talking about the forms of communications data and how sensitive it is, I would say, arguably, communications data is much more sensitive now than it was back then. We have never had the review debate about RIPA. We are only having it now, unfortunately, 12 years later. If we create a legislative framework that is future-proof it basically means that we will never again debate these matters of principle, and that is very dangerous.

David Walker: I agree very much, again, with what Dr Hosein said. If the past and the present are any predictors of the future, it they show that the world changes incredibly rapidly and regarding where we are going to be in 10 years' time, my professional opinion is I have no clue. Therefore, future-proofing a Bill in this way seems to be a fairly futile thing to go at. The only thing that I would suggest could be done to ensure that the text of the Bill stays relatively current with what the world is doing is that when a Bill relating significantly to technology is passed, rounds of post-legislative scrutiny are put in place and commitments made to do that as part of its passing.

Q1026 Lord Jones: I wanted to say, Lord Chairman, thank you to Mr Trefor Davies for his forthright paper, which he submitted in August this year. You say you have a lot of sympathy for those in the area of law enforcement. You went on to say, though, that you have serious concerns that we are going down a path that might better sit in a George Orwell novel. Have you further to add to that?

Trefor Davies: We need to get into the vernacular, then, do we not, in terms of "Big Brother is watching you"? I am not sure that it is a society that we particularly want to live in. Again, it is a difficult one, because I want people to catch crooks. I do not want people to fly planes into the sides of buildings. I think this whole Bill, of all the Bills that we have had in recent years, needs a serious amount of debate, because the judgment and what we come up with at the end has to be based on very informed debate, rather than something that is quickly rushed through because it is perceived that it will provide a benefit, because there clearly are downsides.

I will give you a recent example. It is the first consultation I have ever replied to. I am on the board of the ISP Association and I have always left it to do it, because it has competent professionals to do that. I am not a regulatory person; I am a CTO. But this is the first one I have ever replied to, because I felt strongly enough about the issues. In the course of thinking about it and writing that, for example, I asked taxi drivers. I have had a couple of taxi rides recently, and I said, "Have you ever had anybody leave a laptop in the back of your cab?" I had two taxi drivers who said, "No", but one of them said that in seven years he had had four laptops left, and one of them said he had had eight laptops left in five years. And then when you read the written submissions about the MoD losing laptops and GCHQ having laptops stolen, it does not matter what security oversight aspects you write into a Bill like this,

the information is going to get out in the public domain at some point. I think there will be big downsides in terms of people having their privacy invaded, and you can come up with all sorts of scenarios: somebody might be surfing Alcoholics Anonymous websites or he might have a serious disease that he wants to keep quiet about, or all sorts of personal things. That kind of information will escape. That is really my biggest concern about it.

Q1027 Lord Jones: We do read our papers. We are concerned. You mentioned Orwell; why not read *The Road to Wigan Pier* as well?

Trefor Davies: I did a long time ago ; I have it at home somewhere.

The Chairman: It is because we have all read your papers that you are all here, gentlemen, giving evidence in person.

Q1028 Mr Brown: Have any of you given any thought to what elements might be involved in post-legislative scrutiny arrangements were we to recommend such a thing?

Caspar Bowden: For RIPA or for any Bill that might come out of this?

Mr Brown: For this Bill, if there is to be one at all.

Caspar Bowden: I have to say that I watched the Interception Commissioner's evidence with great interest, and I made a number of points about the Interception Commissioner's role in my written evidence. It seemed to me that the commissioner's evidence vindicated a large number of the criticisms that I made. It does not appear to me that the current commissioner is exercising an effective and credible regime. I do not know what impression he made on you.

I think that I would like to see a much closer connection between Parliament and the oversight and continuous review of any internet surveillance legislation. In particular, in my written evidence, I made reference to a recent European Parliament report that did a comparative analysis of different countries, how they have set up their oversight machinery and their relationship to Parliament. The UK did particularly poorly in that; the European report was very critical of, shall we say, too close links between the oversight role and the executive. That seems to me a syndrome that we indeed have.

Q1029 Lord Strasburger: Might we get a copy of that European report?

Caspar Bowden: There is a URL provided in my written evidence, but I am happy to point you at it, if you wish.

Q1030 Mr Brown: Chairman, could I just ask if any of the others have anything to add? This is uncharted territory, we know that. Is there anything that any of you could add to that?

Trefor Davies: The oversight aspect of it?

Mr Brown: Post-legislative scrutiny.

The Chairman: If there is nothing to say, that is fine.

Q1031 Lord Strasburger: Mr Bowden has argued for a revamped oversight system with a single unified surveillance commissioner reporting to Parliament. What powers and resources would this new commission need to assure you that the use of the legislation was being properly scrutinised and that the necessity and proportionality of requests was being rigorously tested?

Caspar Bowden: I have had the opportunity to do some comparative analysis with the French system and the German system, and there are elements from both that would be worth consideration by this Committee. The French system has essentially a commission. There is no single commissioner with complete authority over that commission. The commission has

itself taken on in the past few years, without statutory authority but with the consent of everyone concerned, the approval of communications data access for counterterrorism cases. It appears to be able to do that with a measure of independence and cost-efficiency, which does not fully satisfy what I would like to see in terms of prior judicial authorisation, but it seems to be much more credible, frankly, than the oversight machinery we have at the moment. They do, for example, emergency authorisation of interception warrants within one hour with independence. They also have arranged 50,000 communication data access authorisations for counterterrorism purposes. They have arranged prior authorisation of each and every one of those. The fully desirable position would be independent judicial authorisation through a magistrate as, for example, now happens with local authorities. I think that could be streamlined and made fairly cost-effective.

Looking at the German system, the G10 Commission is also a mixed commission, but primary parliamentarians sit on it. I think that there would be room for more stakeholders to be involved. I do question the way in which the interception and other commissioners are constrained to be former senior legal figures presently. It seems to me there is a case for allowing people at professorial level with a technical background, but also other qualifications and attributes, to occupy that role. Because, frankly, it does not appear to me that at least those figures who get appointed to the role of Interception Commissioner have been able to understand the technical position, if I can put it bluntly. There is simply no evidence in the way they write reports, in the matters they have covered, or in what they have said in evidence that they are in fact au fait with what is technically involved.

Q1032 Michael Ellis: Can we look at the data from overseas, gentlemen? I notice that both Dr Hosein and Mr Bowden have questioned whether overseas CSPs will accept this legislation, because it imposes legal obligations on them and they are outside the jurisdiction. The Home Office has argued that RIPA already does this, and doubtless there are many other provisions on the statute book, some of which have been on there for many years, which also tend to impose obligations on others outside of the jurisdiction. This Bill will simply extend those obligations to the retention of further data. Do you agree with that, Mr Davies?

Trefor Davies: I do not know, other than if I was approached by an overseas government, I would have to be approached via the channels that we have with our own Government.

Q1033 Michael Ellis: Do you think that there will be a problem with organisations outside of the jurisdiction accepting this English legislation?

Trefor Davies: Why would they want to accept it?

Dr Hosein: We have consulted with almost all of the large providers, because the Home Office told us exactly the same thing, which is that foreign CSPs already fall under RIPA, and I was surprised, because I thought I must have been wrong for the past 12 years. When I went to these foreign providers, some of them laughed in response, again, saying, "That is just not true". And then when we looked into it, the reason the Home Office would say that is because if it was not the case that the foreign CSPs were under RIPA—

The Chairman: I need to suspend. There is a Division in the Commons. We will reconvene as soon as we are quorate with Members of the Commons.

Sitting suspended for a Division in the House.
On resuming—

Q1034 The Chairman: We are back in session again, and back on the record. I would be grateful, Dr Hosein, if you can remember Mr Ellis' question, if you would start from the beginning in answering it.

Dr Hosein: I do. The Home Office states that foreign service providers fall under RIPA because it has to. Otherwise every request that the Home Office has placed under, say, Google or Facebook would be illegal or beyond the law. The situation for foreign service providers is that they voluntarily reply to some requests. They do not reply to all requests; they reply voluntarily to some requests. Their preference would be that the requests would go through mutual legal assistance treaties, because the challenge they face, particularly those who are based in the United States, is that the standard of law in the United States is far higher than the standard of law in the United Kingdom.

Q1035 Michael Ellis: Are you a lawyer?

Dr Hosein: I am not a lawyer, but I have consulted with all the lawyers I could on this matter. I have consulted with lawyers who are fighting this case in the Supreme Court right now with the National Security Agency and the Bush Administration and the Obama Administration.

Q1036 Michael Ellis: So is it your position, Dr Hosein, that the Home Office is lying?

Dr Hosein: I am not saying they are lying. I am saying that they have to say that in order for their requests to be compliant with RIPA.

Q1037 Michael Ellis: Hold on; I am going to press you on this, because you are effectively saying the Home Office are lying, aren't you? You are saying that they are saying one thing and mean another thing.

Dr Hosein: I am not saying they are meaning anything else. I am saying that they have to say that in order to be compliant with RIPA with these requests. Otherwise they are making RIPA requests against an organisation that they cannot make requests against.

Q1038 Michael Ellis: There are plenty examples, are there not, of cross-jurisdictional cooperation, not only in this sphere but in many different spheres. For example, the United States frequently imposes obligations, does it not, on other countries that they have to comply with, at least if they want to do business in the United States. Is that not the case?

Dr Hosein: Yes, that is the case.

Q1039 Michael Ellis: It is becoming increasingly common for countries to enact legislation that imposes a burden on other countries. Why do you not see that working in this case?

Dr Hosein: I believe that this Parliament can choose the passage of legislation. I just do not believe that the foreign providers will look upon that favourably or comply.

Q1040 Michael Ellis: Please, gentlemen, you can join in. If the Home Office are saying to the contrary—they are being told something different from what you are being told by providers—what would you say about that?

Dr Hosein: In the discussions we have had with providers they say they respond to requests on a voluntary basis.

Q1041 Michael Ellis: What I am saying is the Home Office's position is that providers will co-operate with them and therefore they do not envisage this problem that you are concerned about. Do you have any reason to doubt that or refute it?

Dr Hosein: My point is that they voluntarily.

Q1042 The Chairman: Could I pursue this point, Dr Hosein? You said initially that when you took this up with the foreign service providers they just laughed at the concept. Did you find any inconsistency between the views of, say, the London head office of those American providers and the American head office?

Dr Hosein: No, I did not. I did not see any difference between the London office or the foreign offices of these providers.

Q1043 The Chairman: The head office in the States. That is interesting, because I think we were getting suggestions that the evidence we got from our CSPs in the United Kingdom that there would be potential difficulties with this was not the case, because the Home Office had assurances from the HQ in California. Can you cast any light on that?

Dr Hosein: The conversations we have had with senior legal officials in the US is that they want to help—they really do—but the problem, once you start placing legal obligations, is that if the United Kingdom does it then the Saudi Arabian Government will do it. How do you pick and choose between governments? It creates an awkward environment, so therefore that is why they prefer a voluntary arrangement where they pick and choose which requests they respond to. Secondly, they are far more favourable towards the legal route, the pure legal route, which is compliant with law in the requesting country and the requested country. In the United States, they would like to see it go through the mutual legal assistance treaties that require requests to go through the courts in the United States.

Q1044 Baroness Cohen of Pimlico: When we were talking to the Metropolitan Police, it was clear that the biggest of the foreign service providers most certainly picked and chose. For example, they co-operated unhesitatingly if it was murder or terrorism. Certain other forms they refused, if they did not feel that it was particularly appropriate. Obviously our Home Office hope that if this legislation went through, it would stop them picking and choosing, and that they would decide to co-operate fully with whatever request. What would your view be on that?

Dr Hosein: My opinion is that we are on a collision course. They are relatively happy with the voluntary regime. The moment there are arduous provisions placed on these companies to do something based on the decision of a parliament in another jurisdiction they are going to start saying, "We will not reply. We will not respond." That is why I am very surprised that the Home Office is choosing to rock the boat. I do not like the voluntary arrangement at all. I believe in the rule of law. I believe requests must follow some framework established by Parliament, but the Home Office is rocking the boat over this voluntary, slightly dodgy, legal arrangement—or not necessarily strongly bound arrangement.

Q1045 The Chairman: Anyone else?

Caspar Bowden: I do have slightly different observations to make. I have referred to a problem in my written evidence that I call "schizoid jurisdiction". This occurs when an international provider decides to respond, say, to a RIPA Part 1, Chapter 2 request or demand for communications data and they fulfil this through their local office and they give this to the local law enforcement agency, exactly as would occur with a domestic communications service provider. But when a data subject—an individual—makes a request to exercise their privacy or data protection rights, then the company will say, "Oh no, I am sorry. That data

was transferred to the United States", and now falls under something like the Safe Harbor Agreement where, in practice, the individual's rights are much less. So I am a little bit confused by this language of voluntary compliance. I think now all reputable communications providers, whether they are international or domestic, respond to RIPA Part 1, Chapter 2 demands for communications data, so it is not voluntary in that sense. The question that Gus, I think, correctly raised is it is not just the UK that is going to be wanting this. It is going to be Indonesia, it is going to be India, it is going to be regional powers, and all the time there are a few big global providers.

Can I just pursue this and try and break down two aspects in answer to Mr Ellis's questions? When we talk about the foreign provider complying, what exactly do we mean? Do we mean that they will be keeping data types, which they do not ordinarily keep, in response to some voluntary request from the UK Government? Or, in particular, do we mean that they will be responding to requests to the so-called filter that somehow they will provide an interface into their systems, typically in the United States, to allow data mining of very general kinds within their own body of data? That seems to me extraordinarily unlikely that that will occur. Then, to go back to the first question, about whether any international company will retain data types that they would not ordinarily retain, that also seems to me fairly dubious. I would be surprised if any general counsel of a US-based company has given such an assurance to the Home Office. I would find that surprising.

Q1046 Lord Jones: Gentlemen, this is on third-party provisions. There has been criticism about this, and I think Dr Hosein has made some criticisms perhaps as recently as July. Some of you have expressed considerable concern about the proposal to ask UK CSPs to collect third party data. The Home Office has not conceded that it might be necessary to write assurances into the legislation, firstly that the original data holder would always be contacted first, and secondly that UK CSPs would not be asked to store or release encrypted data. If these assurances had legislative backing, would they allay your concerns?

Trefor Davies: I am not really sure that it makes any difference whether it has legislative backing or not, because the reality is that it is a lot easier for this third-party data to be sourced from the third party rather than from the ISPs themselves. But I would imagine—and I do not have numbers—that a vast proportion of this third party data would be encrypted. Therefore, in order to be able to access it we are into that debate again about the technical feasibility of it. I recognise that in the written evidence there were a lot of different level-playing-field issues and legal and commercial issues, but from my point of view it is the technical practicality of it.

Dr Hosein: It is still a form of coercion to tell a foreign provider, "Comply with our request or else your client's data will be stored by a third party in a foreign jurisdiction". You are putting the provider in the middle of a rock and a hard place, and that is the intention of this very approach. It is, "Comply with us or we will make sure there is a domestic pool of the data of your users", and that is highly problematic. I think there is a way through this. It is not for me to recommend policy, but what your question seems to be pointing to is that there are very specific targets that the authorities in this country want to know more information on, whether it is internet places or individuals, and that allows for the type of regime that Mr Bowden talks about, which is a targeted presentation regime, in which you can ask for a national-security-level concern that ISPs in this country would monitor traffic to a specific provider, but in a very specific circumstance, under a very specific authorisation. While there are issues of debate around that, I believe that that is a more proportionate response than going to all the foreign providers and saying, "Do what we say or else".

Q1047 The Chairman: But the Home Office, I think, would say to that point that that is all very well if it is an ongoing operation: you have a potential terrorist, X. "Can we please preserve everything on this guy until we have enough evidence?" That is a different situation from when they come across terrorist Y and then they say, "Can we see what you have?" and we have not been storing anything on him. So you do not provide the whole answer.

Dr Hosein: Addressing one slightly different aspect to that, imagine there is a social network for terrorists based in Malaysia—a service provider that runs a social network for terrorists—and we want to be able to monitor all the terrorist activity and terrorist users who may be based in the United Kingdom. There would be a way to have targeted preservation of traffic going to that specific resource. That is very different from requiring all resources on a "Do what we say or else" regime.

Caspar Bowden: I would agree and develop what Dr Hosein has said. I think what we are asking is for law enforcement to look at their task progressively in a different way, which is instead of assuming that somehow there can be blanket recording of this data about the entire population, it is going to be more of a question of beginning, as it were, with the threads that are available and then developing an investigation. You would widen the circle of interest and cumulatively broaden the use of the powers of preservation until you were in a position to acquire the evidence and intelligence you need. This could be something of an upheaval for the way law enforcement has proceeded so far and I think this must be accepted, but honestly, we have to give data preservation a chance. We have to develop a credible regime with which law enforcement can live to try and make this work before we go to the stage of saying that somehow it is acceptable to perform this blanket preservation on everybody in the entire country.

I will offer, perhaps, a slightly dramatic example of how far we have come in 10 or 15 years. In communist Albania, the secret police, the Sigurimi, used to have a ritual where every year they would require every citizen to come and have a chat with their secret police. Each person would be required to co-operate in building what was called a "biografi". This was, as it were, a personal dossier in which they would have to record all of their social relationships, social contacts and main meetings that had happened to them over the previous year. In terms of the way we live our lives now, particularly the way in which social relationships are expressed, through the internet, we are effectively allowing the Home Office to build a biography on everybody in the country on their pattern of social relationships and on the fabric of everyday life. It seems to me, just taking a step back, it is extraordinary that we have got to this situation at all and we are even contemplating it.

Q1048 Craig Whittaker: Mr Bowden, can you honestly believe for one minute, though, we are talking about an Albania situation here in the UK? We are not talking about building a profile. We are talking about securely storing information. The profile-building, if you will, will be in the access and the safeguards put in place to get that access. I think that is a little bit scaremongering, from that point of view.

Caspar Bowden: With respect, not. Look at the testimony of William Binney; I also referred to in my written evidence, and his video to a hacker conference in New York is available online. William Binney was a senior National Security Agency engineer who has now become a whistleblower, objecting to these types of practices conducted in the US. The technology that he, as a senior engineer, was building 10 years ago was in fact precisely an automated biography file; it was not merely a question of leaving this data passively in place. And there is a direct correspondence between the sort of machinery that he engineered 10 years ago and what is proposed in the filter. Of course, it depends exactly how the filter is going to be implemented and what lies behind the filter, but I do not think it is correct to

imagine that somehow these are, as it were, passive piles of data sitting around. Even if that was the case, there is certainly case law at the European Court of Human Rights to show that blanket retention of this kind of data, particularly if it is going to be used for pattern analysis and traffic analysis, is well beyond what the European Court has tolerated so far.

Trefor Davies: Just to add, I think we are kidding ourselves if we think we can keep everything secure. You only have to look at the recent case of the chap who hacked into the Pentagon computers from his back bedroom.

Q1049 Lord Armstrong of Ilminster: Changing the subject to the definitions of subscriber data, user data and traffic data—as you might say, the RIPA definitions—the Home Office said, when we saw them the other day, that it might be sensible to reconsider these definitions in order to allay fears that information not traditionally considered as data could be caught by the legislation. What I wonder is whether you think that narrower definitions of communications data or revision of the existing communications data would allay some of your fears about the scope of this Bill?

Trefor Davies: Would you care to suggest what the narrower definition is, because I am not sure that I could?

Lord Armstrong of Ilminster: We are asking you.

Q1050 The Chairman: Perhaps one example may be on subscriber data. At the moment, subscriber data is everything else that remains, which could be, if one was on Facebook, up to about 78 different items. Subscriber data has expanded dramatically since 2000, when it was my name, address and my mobile phone number. Now it could be everything that was on my iPhone, if I had one. That is just one example, possibly, theoretically, where one could say "subscriber data in future will only be X, Y, Z".

Caspar Bowden: I did watch some of the recent evidence sessions where this question was also discussed and particularly the Facebook issue of whether your favourite colour or favourite X, Y, Z could technically qualify as subscriber data. I think it would be a modest and useful restriction to ensure, for example, that that was not possible. However, the way in which we have arrived at the current definitions of the three main categories, it should be borne in mind, goes back to 2000 when RIPA was being debated in the House of Lords and, essentially, the House of Lords lost confidence that the Home Office knew what they were doing, and the definitions of communication data had to be rewritten with some urgency between second reading and report stage.

Industry had some input into that, but I do not think there was much civil liberties input into that, so the definitions we have today have various anomalies. For example, the record of itemised phone calls that one makes outbound from one's phone currently falls, if one looks at the Code of Practice, into the category of use data, whereas incoming phone calls, which of course the individual does not necessarily see, falls under traffic data, but their impact on privacy is similar. Therefore, I think there would be scope for rationalising the definitions to try to reach some equivalence in their privacy impact, which is the correct way of analysing this, in my view. Most of all, I think one should try and separate the concept of traffic data, in a broad sense, from subscriber data. Subscriber data is essentially static and deals with the identification of people. Traffic data deals with your social relationships, what you are interested in, and what is really going on inside your head. This is intrinsically far more privacy-sensitive and should be dealt with, in my view, much more under the rubric of interception, because the impact on privacy is analogous.

David Walker: While I see that clarifying the characterisation of these data types would be extremely useful from a legal perspective, there is a considerable technical problem that these classes of data are very intimately mixed in the communications themselves. To

use Mr Bowden's example, when it comes to mobile phone calls, the mechanism by which the text messages we are used to sending and receiving on our mobile phones pass from one handset to another uses the same signalling mechanism that is used for ringing someone up. Again, in terms of capturing that data and logging that data, separating them out as part of a capture process is going to be extremely hard, especially given the vast proliferation of protocols in existence.

Q1051 Craig Whittaker: Dr Hosein and Mr Bowden, you have advocated a warrant system, and I think you said it would apply to all agencies wishing to access the comms data. As a Committee, we have heard and taken evidence that the current SPOC scenario and authorising officer system is much more expert and rigorous than a magistrate necessarily would be in a warrant system. Do you accept that might be the case?

Caspar Bowden: In my observation, SPOCs do play a useful role. If one looks again at the current Code of Practice on acquisition of traffic data, the various roles of SPOCs include giving advice and trying to ensure consistency within a particular organisation, and all of that should continue and is necessary. The problem is one of the principle of independence. The authorisation to access this data, as we have covered, can be highly privacy-intrusive—as intrusive, I would say, as interception—and should be done through prior judicial scrutiny. Now, I do not think it is going to work to somehow imagine that one can keep a system that would assign these authorisations to some random magistrate. I think we should consider, together with a reformation of RIPA, how we can organise essentially a specialist magistracy to triage and deal with these in an organised and efficient way and, preferably, to try to put interception of communications also on a basis of prior judicial scrutiny. There would be the opportunity to do two for one, and to have the same sorts of work dealt with by the same sorts of magistrate, but they would obviously be dealing at different levels of justification or suspicion. So to justify interception you would need a more serious and more detailed case than to initiate the preservation of certain sorts of communication data.

Q1052 Lord Armstrong of Ilminster: When you say "interception of communication", are you referring to the Secretary of State warrant system?

Caspar Bowden: Yes, I am. I am personally not happy with the Secretary of State system for a number of reasons, but I will not digress that way. I would take the opportunity to consolidate both, ideally. I did notice, re-reading the Code of Practice, that there is a curious self-imposed limitation in the way in which Part 1, Chapter 2 authorisations for communications data are currently applied, which is if a law enforcement agency wants to secure data about the future and to record data, which would not, perhaps, otherwise be recorded, about future communications, the Code of Practice says that can only be done for one month. This is very peculiar. There is no statutory reason or human rights reason why that should be limited to one month. One might think it is almost the Home Office trying to not use preservation very much because they regard retention as such a valuable tool and they do not want to upset the status quo, which accepts the retention regime. If one moved to a prospective positive, targeted preservation regime, then obviously you would want to authorise the future retention of data for a longer period.

Q1053 Craig Whittaker: Just for clarity then, you are talking mainly about the Secretary of State system. What about a run-of-the-mill SPOC system? I think you were advocating earlier on that we should have a warrant system.

Caspar Bowden: One has to say what one means by a warrant, because at the moment, for interception, a warrant is issued by the Secretary of State. I do not favour that approach. I am talking about a warrant, as it were, issued by a judge or a magistrate.

Q1054 Craig Whittaker: Yes, but I am particularly asking about the system we currently have in place for the accessibility to the data on a much lower level.

Caspar Bowden: As I set out in the written evidence, my own position on this is that provided that subscriber data was limited, in the way the Chairman suggested, to quite narrowly defined types of what we would ordinarily consider subscriber data, I would be content for SPOCs to authorise access to subscriber data. I would say that anything that is traffic data or usage data, which is intrinsically far more privacy-sensitive, should require a magistrate.

Dr Hosein: I am highly sympathetic to the SPOC system as an integrity check and I believe it is a very good stopgap measure for that, but I do not believe it is sufficient for a true test of necessity and proportionality. That is why you need independent oversight. The reason we all like the SPOC system is because the SPOCs are trained. They have knowledge about the technology and about the law. The reason we are currently suspicious of magistrates and judiciary is that we doubt they have the capability. I find that very worrying. If we are concerned that the judges in this country are incapable of understanding the complexity of these types of request, that is something that needs to be fixed beyond the scope of this law.

Q1055 Craig Whittaker: We are not talking about the judges; we are talking about the magistrates.

Dr Hosein: Even so, we would still need to address that issue, because it already exists under the Protection of Freedoms Act that magistrates are involved in some authorisations, particularly from local councils and whatnot. If we believe they lack rigour to respond to these types of requests, how come we authorise them to do so under the Protection of Freedoms Act? I believe that our judiciary and the magistrates may need training at the same level that SPOCs do. SPOCs are a good example of what happens when you train people appropriately.

Q1056 Craig Whittaker: Can I just get you to clarify why you feel that a warrant system needs to be in place above the SPOC system, which appears to be working quite well?

Dr Hosein: The SPOC system may notice errors and may notice some abuses, but the SPOCs look at whether something is lawful. They are not necessarily the arbiters of what is necessary and proportionate in a democratic society. That balancing test between the public interest and individual liberties has always resided with an independent body.

Q1057 Craig Whittaker: Would it help if we put the SPOC on a statutory footing, like we do with those designated senior officers, for example? Do you think that would help the situation?

Dr Hosein: I do not believe it is sufficiently independent. As Mr Bowden was pointing out, communications traffic data is becoming even more sensitive than communications content. One opportunity for this Committee is to start having a debate about why is it we protect communications content to such a degree but not highly invasive data-minable communications data and why are they any different? I believe once we start having that debate, we will start asking why is it we require a warrant for content but not for communications?

Q1058 The Chairman: We are in interesting territory, and I think the Committee generally picked up that the best trained SPOCs are very good and that system seems to be working. The question is about what level of oversight of the SPOCs, and the type of

oversight, whether judicial or a commissioner or whatever, is required. That is what the Committee will be agonising over.

Caspar Bowden: I just wanted to make the point that looking at the evidence the Committee has received and my own researches over several years—and I do not know what evidence the Committee has received in private—it is still not clear to me what criteria SPOCs use to determine what is necessary and proportionate. Indeed, it is not clear what criteria the commissioner uses, despite his evidence. If one wants to get down to concrete cases and say for a mugging or for a murder 5,000 people's data will be accessed, or 50,000 people's data will be accessed, one needs to have some concrete yardstick of really what is being done, and I have no idea. I do not know if the Committee has managed to unearth that sort of practical information. I noted the Interception Commissioner, in his evidence, said he does not have any difficulty deciding which is which, and I suggest this would suggest this means that all SPOCs are somehow operating with some sort of magical sense of pre-established harmony, which I find rather hard to believe. I would like to know concretely what is considered necessary and proportionate. I do not think the SPOCs have the independence to really do that in the same way that a magistrate would.

Q1059 The Chairman: That is an interesting point, which the Committee will be exploring.

Trefor Davies: Just to add, we get RIPA requests, but we do not get very many, maybe one or two a year. By and large, the quality of what we have been asked to do seems to be acceptable and they are genuine right requests. What I did pick up, though, in the written submissions and the written evidence was the Big Brother Watch submission regarding the variations in the way these requests are made. Kent Police, in two years, made 7,664 requests for data with 3,237 of those rejected internally, compared with Merseyside, who made about 30,000 requests and only 500 of them were rejected. It does make me raise an eyebrow a little and ask whether the oversight is really overseeing.

The Chairman: That is an interesting question to which I personally do not know the answer at this precise moment.

Q1060 Baroness Cohen of Pimlico: Can I just sort out in my mind that Mr Bowden divides subscriber data from traffic data—we all do that—but in terms of subscriber data would be perfectly happy with a SPOC.

Caspar Bowden: One has to bear in mind that the Code of Practice does not exclude other interpretations. In fact, I wanted to draw attention to this, as reference was made a couple of evidence sessions ago to the way in which the Code of Practice, shall we say, takes care of these things. If one reads the Code of Practice, it says "the sorts of data falling within this category include", so the Code of Practice by itself does not exclude far-fetched or over-expansive interpretation, so I think it is useful and necessary to have very precise definitions in primary legislation that would exclude far-fetched interpretation.

Q1061 Baroness Cohen of Pimlico: If we could get the subscriber data definition satisfactory, you would not feel that needed a magistrate. You would be happy with a SPOC doing that. I do not mean to put words in your mouth; I am trying to check.

Caspar Bowden: With other qualifications, that is broadly my position, because I think that represents something that is doable. That would have to be done, in my opinion, with a move towards a preservation methodology by law enforcement.

Q1062 The Chairman: Dr Hosein is going to say that is provided someone is second-guessing "necessary and proportionate".

Trefor Davies: Yes.

Q1063 Baroness Cohen of Pimlico: That was my next question: even for subscriber data you still feel that.

Dr Hosein: I understand that the mood in this discourse has moved that subscriber data is not as valuable, but as a privacy advocate, I have to remind people about the protection of journalists, the protection of journalistic sources, and the protection of leak sources; the revelation of subscriber information will reveal all of that, and so even that needs an independent test of some sort.

Q1064 Stephen Mosley: We have heard diametrically opposed views on the filter. On the one hand, I know, Mr Bowden, you have described it as a "hyper-Orwellian menace", while the Home Office would let us believe it is a way of protecting people's privacy by eliminating people who they are not interested in. I guess it could be either, depending on how it is used, so the oversight and the control of the filter is going to be incredibly important. What kind of oversight do you think the filter should have to ensure the protection of people's privacy?

Caspar Bowden: Perhaps it will not surprise the Committee to say that I do not think the filter should be built under any circumstances for domestic surveillance. It is understood that GCHQ have had these sorts of capabilities for many years for international communications, but I simply think that the kind of capabilities described in the filter are intrinsically incompatible with a modern democratic society—on the basis of blanket data retention, you understand. If we are talking about preservation of data about designated targets, where for each designated target there is a reason and a justification—even if that is a reasonable belief or a reasonable suspicion—that is still a far smaller 1% of data than one would be talking about on the basis of blanket retention. But for anything to do with the so-called filter—I would call it data mining—of particularly traffic data, which is so prejudicial to private and intimate life, I think safeguards and oversight are irrelevant. I just do not think it should be done in a democracy.

Q1065 The Chairman: Does anyone else wish to comment?

Trefor Davies: I agree.

Q1066 Stephen Mosley: Turning to you, Mr Davies, then, if this filter does come in, a company such as yours will have to interact with the filter and use a standard data format; I know we have been told about RDHI, etc. As a business, would that cause you any problems at all?

Trefor Davies: There is almost certainly going to be an overhead with running and interfacing it, aside from my concerns about whether it should be there or not in the first place. The biggest problem we would have as a business is the amount of effort that we would have to put in, in the first place, to setting it up. I will give you an example: as a business, we are not a small ISP anymore. We have about £40 million turnover, we have a couple of hundred staff and maybe 40 of those people are engineers, but most of the engineers work on day-to-day customer-facing stuff solving problems. The real core of our team who would have to work on this kind of stuff is only six people, and they are network engineers, systems engineers, and applications engineers. We have some deep packet inspection equipment, which we installed two or three years ago to protect our customers' networks from surges in traffic, and we had to have a couple of engineers working for about three to six months on that full-time, with an external contractor, to install it. For us, there was a business case for doing it.

We have six engineers. Smaller ISPs may only have six or 10 engineers to do what we do with 40 or 50 engineers, but it would still take the same amount of effort, so the smaller the ISP the more disruption and harm it makes. It is not a great leap of imagination for me to believe that if I was having to implement the systems to interface with the filter then I am probably looking at half or two-thirds of my development resource, which I then would not be able to have working on my next products, bringing the business into the 21st century with virtualisation and the cloud. Every ISP in the country is racing to try to bring out new products to keep up with the technology, and it really would have a big impact.

Q1067 The Chairman: Are there any outstanding points? I think we have concluded our evidence session, gentlemen, unless you have any other concluding remarks to make.

Dr Hosein: Just one sentence: please do not drop the issue of notification. I will remind you of a case in Poole of the family that was placed under surveillance by the council because of catchment areas. The only way the family was notified of the fact that they were under surveillance was because the council accidentally told them. People need to be informed of when they are placed under surveillance when it is no longer relevant to the investigation or harms any judicial processes.

The Chairman: That is a legitimate point. I have curtailed our discussions today because we are running out of time, but we are grateful to you, in particular, Dr Hosein, for that evidence on notification, which we are considering in written form; thank you for drawing attention to it. Gentlemen, we are very grateful. Thank you very much for coming here today. Thank you for your written submissions initially, which provoked us into bringing you forward to give oral evidence. Thank you very much.

Examination of Witnesses

Witnesses: **Steve Higgins**, Detective Superintendent, National Policing Improvement Agency, **Sir Peter Fahy**, Chief Constable of Greater Manchester Police, **Peter Davies**, Chief Executive, CEOP, **Alan Lyon**, Detective Superintendent, Greater Manchester Police, and **David Stevenson**, Detective Sergeant, Accredited SPOC Manager, PSNI, examined.

Q1068 The Chairman: Welcome to the afternoon session. I am sorry we are running slightly late, gentlemen, but you are very welcome here this afternoon. Whilst we all know who you are, I would be very grateful if you would just say who you are and who you represent, for the record, starting with Mr Higgins.

Steve Higgins: Detective Superintendent Steve Higgins. I represent the National Policing Improvement Agency. I also sit on the ACPO Data Communications Group Executive.

Sir Peter Fahy: Peter Fahy, Chief Constable of Greater Manchester Police.

Peter Davies: Peter Davies, Chief Executive Officer of the Child Exploitation and Online Protection Centre.

Alan Lyon: I am Alan Lyon, a Detective Superintendant at Greater Manchester Police and the Senior Responsible Officer for communications data.

David Stevenson: David Stevenson, Police Service of Northern Ireland, SPOC Manager and also the Secretary to the Data Communications Evidence Subgroup.

The Chairman: Excellent. Thank you very much. We have a lot of questions to get through in the time. We will probably run slightly late with you as well. Do not everyone feel you need to answer every single question. If you feel it has been covered by a colleague, then we move on.

Q1069 Dr Huppert: Can I start off with an apology to Mr Davies for not having been with him just before this at another Select Committee, but credit to myself for trying to be in two places at once? The Government has identified two specific types of data that it wants the UK CSPs to retain; it announced this at a session last week. These are data relating to allocation of IP addresses and weblog data—the information up to the first slash. Are you aware of a data gap existing, specifically in these areas, which you think needs to be addressed so that your organisations can perform better?

Sir Peter Fahy: Certainly, as Chief Constable in an area with a serious problem of organised crime in particular, I think the way I would describe this is that often when you are carrying out these sorts of investigations what you are trying to prove is associations. Sometimes this is obviously an association between an offender and a place or an offender and a victim, but often it is associations between different groups of criminals. For instance, if you arrest a foot soldier, in effect, who is delivering drugs and you are trying to prove an association and trying to capture the higher-level drug dealer, then clearly you are trying to prove that association. Up to now, we have been able to use some of the more readily available communication data to do that. But the fact is we are seeing that the criminals are realising that, moving to some of the new technologies and platforms, and really what we see is obviously, as most people do, an explosion in those new technologies—the new apps—and clearly we are very fearful that we will quickly lose the capability to do that. We already have specific examples of them using some of those new platforms to defeat us.

Q1070 Dr Huppert: Sir Peter, the Home Office said last week that the two main issues were IP addresses and weblog data. Are you saying you disagree: that those two would not resolve it?

Sir Peter Fahy: No, they absolutely would resolve it in terms of starting to capture some of the other forms of communication that we know that those criminals are starting to use. Again—I know you accept this point—it is not about the content of those communications; it is the fact that you are communicating with this other person, which then starts to create the relationship and then we can use other data to prove conspiracy.

Q1071 Dr Huppert: In your experience, do you have a sense as to how important each of those two categories are? Which one covers more of the gap?

Sir Peter Fahy: No, I think they are both equally important and equally responsible in terms of crime investigation and proving that case. But it is fair to say that we are very aware of the way that the technology is developing and therefore, clearly, we need to try and maintain that capability and try to make sure the legislation is framed so that it maintains that capability for the months and years ahead.

Q1072 Dr Huppert: If the legislation were just to specifically restore those two capacities, that then would satisfy the majority of your concerns about the data gap, is that right?

Sir Peter Fahy: I think it would presently. I think we have to be clear, as everybody is, that trying to forecast how technology will develop is very difficult. What is concerning us is that we are continuing to see people offer ways around some of the existing technologies and some of the existing techniques that we use. I want to be realistic with the Committee to say that, clearly, when you look at the way that some of these people are developing, when you see what is being offered—and of course when it is on the net it is available internationally—then I would not want to say that if you provided this and the legislation

went through then suddenly the problem would be solved for so many years hence. I do not think anybody could say that.

Dr Huppert: Okay, but it would solve the current one.

Peter Davies: As I know you are aware, we approach this from a slightly different angle. Some of what we deal with at CEOP is serious organised crime. Some of it is more internet-dependent than other bits, but we also deal with protecting children who are vulnerable and at risk, and often the only opportunity to identify them is through communications data. I do not think I can tell you which of the two options you give us are the most prevalent in terms of IP addresses and weblog data. However, I think what needs to be acknowledged is the need not to frame legislation just to meet the needs of today, but to frame legislation that is capable of dealing with the developments in technology of tomorrow. So, from my point of view, our type of offenders—our predatory paedophiles—are online and are among the most sophisticated there are.

Q1073 The Chairman: I am sorry, Mr Davies, but how on earth can we frame legislation to meet the needs of tomorrow if we do not have a clue what those things are going to be?

Peter Davies: I think the fundamental things about communications data do not change. They are a transfer of data between point A and point B, the opportunity to identify point A and point B, and the opportunity, having done so, to understand what point A, as an account, is doing, provided the legislation enables us to do that. Those are pretty much the same issues to do with comms data.

Q1074 The Chairman: With respect, could I disagree on one point? I sat on RIPA in 2000, and in 2000 my mobile phone would give you basic subscriber data, the number I called from and the number I called to. Now my mobile phone tracks me every inch of the way, and every five minutes you have a record of where I am, and that is with most people. That is quite a fundamental change between what you are capable of doing now and what we envisaged in RIPA in 2000. I am merely suggesting to you that to make something future-proof means it is totally open-ended and may be undemocratic.

Peter Davies: I appreciate that. I know you will probably explore this in the rest of your questions, but the alternative risk is that you make something that is adequate for the needs of today but does not help people protect the public or investigate the serious organised criminals of two to three years' time. I am not sure that legislating after the fact on a pretty continual basis, which is what I think would be required to reflect the developments in technology, is a better option.

Q1075 Dr Huppert: I understand the point you are making and future-proofing is an issue we have discussed a number of times at this Committee and how one does it and how one ensures parliamentary and democratic oversight, but can I just make sure that I understand in terms of the current problem. As you say, you have a different set of issues that you deal with. Would these two things solve the majority—or the vast majority, ideally—of your current problem as well as Sir Peter's current problem?

Peter Davies: I think they would solve the majority of our current problem, yes.

Q1076 The Chairman: Is it the Committee's view that what you want 99% of the time is who talked to whom, when and, possibly, from where?

Sir Peter Fahy: Yes, absolutely. As I say, what is crucial is to be able to prove associations and, in particular, in things like organised crime, to try to be able to capture the people further up the tree so that we are taking out the more serious offenders.

Q1077 Baroness Cohen of Pimlico: The other bit of the gap that the Home Office tell us they want to address is data from the overseas CSPs. We understand there are two sides to this problem: some overseas providers do not retain the stuff at all, and some of them do not respond quickly or, indeed, possibly, at all. Can you tell me, all of you, how much of a problem that is, in your experience?

Sir Peter Fahy: Again, it is a significant problem, and it is about the two things that you said. It is sometimes the time delay. There are certain providers that are pretty obstructive and are uncooperative. We had a case around Christmas-time where we were up against the custody clock; we have arrested somebody, we are trying to do an investigation, and we are trying to get enough evidence to get them charged. The international processes are just incredibly, incredibly slow. It is obviously the issue that the internet is international. Often it is not just about us investigating. We then have to do disclosure, so it may be that we have to cover this particular line for the defence as well, and the MLAT procedure, as it is called, we find can be very, very slow. But it is also this issue that some providers are very cooperative, while other providers are essentially obstructive and do not recognise the need. Therefore, clearly, it is important that this legislation, as far as it can, tries to cover that.

Peter Davies: I am backing up what Sir Peter says. This is not an overwhelming problem for us at the moment, but there is every indication, I think, that the ownership of the internet and, therefore, the location of communication service providers, will migrate to other parts of the world. At the moment, where we have good relationships with US service providers and they are subject to some legislation that places an obligation on them to report child sexual exploitation that happens on their networks, the situation is really good or reasonably good. What we need to do is provide for the likelihood that it will not be as good when larger portions of the internet are owned and operated overseas. It is a containable problem at the moment, but there is nothing about it that seems inherently stable, and it may well be a far bigger concern for my centre in the next year or two years.

Q1078 Baroness Cohen of Pimlico: Do you find that the co-operative ones answer all your requests, or do they pick and choose?

Peter Davies: They answer the ones they can, when they can. I think the level of retention and responsiveness is different with each provider. There are some providers that do not have a business need to retain the data, and therefore do not retain it and it is a pretty well articulated fact that roughly 25% of comms data requests currently do not come back with any information. The risk is that that might increase as a proportion quite substantially. I can go on to talk about what that means in practical terms.

Q1079 Baroness Cohen of Pimlico: I am prodding because of your particular field, but we were told by a previous witness that many overseas providers co-operated unhesitatingly if it was murder or terrorism, but for harassment and internet bullying they would not bother.

Peter Davies: We do not deal with harassment or internet bullying. We put people onto those who do. We deal with serious-end sexual exploitation of children by a variety of means. That generally galvanises people.

Steve Higgins: There are two key issues here. One is the speed of the response. We have a system in the UK where automated solutions within the companies for the recovery of the data has significantly improved response times as against a manual process. I think one of the benefits of the Bill, were it to be passed, would be that it would potentially facilitate investment to enable that to take place. That is one of the issues.

The other issue, of course, is that no matter how cooperative an overseas company may be, if they do not have a data retention policy or requirement in place in that particular jurisdiction, no matter whether it is MLAT or any other process, they simply cannot provide us with the information. So it is the ability to work with them and enable the retention of that data.

Q1080 The Chairman: What about their willingness to disclose? I think Mr Davies said there is a 25% nil return. Is that all because they do not have the data? How much of that 25% is because they may have it but they are not happy to disclose it, because we have not gone through legal means or whatever?

Peter Davies: It is difficult to tell sometimes. It is slower to get disclosure for evidential purposes than for intelligence purposes. That is a distinction. I think almost anything is technically possible if there is sufficient will to do it, and so the issue about what it technically possible crosses over into the issue about what people have the will to do. Each of our relationships with each of the service providers is different. They have different strengths and different areas for development. That is one of the frustrations of what we do, because if there was a consistent level of expectation about retention and access to this data, the extent to which we have to cultivate those individual relationships and, to some extent, hope for the best would be significantly reduced.

Q1081 Craig Whittaker: Just on what you have said there, do you think making retention of third party data over here from overseas, for example, is going to make any difference to that at all? Because we have heard very clear evidence that a lot of companies will encrypt the data, so it will not be able to be used here, so you will still have to approach a company directly overseas yourself using a different method.

Peter Davies: I am not so familiar with what companies will or will not do. I think it depends on what expectation is placed on them by legislation. Let me be clear. The operational ideal, probably for CEOP, but certainly for anybody involved in dealing with serious and organised crime in any of its forms, would be that any level of communications data that is criminal-related within the UK is capable of being researched to the point of identifying the point at which it left to the point at which arrived and proving the traffic between the two points. I am not so familiar with that issue about third party data, but we would want that to be held within the UK and accessible within the UK, because if that cannot be provided then it is probably lost and, for reasons I mentioned before, that is a significant risk in terms of our ability to use this information to protect people and pursue criminals.

Q1082 The Chairman: You said they might co-operate depending on the legislation imposed on them, but we can pass, in the United Kingdom, legislation that we can impose on British companies or companies operating here. Regarding some of the American giants—and we all know who they are: companies that launched with maybe $100 billion turnover or value and are now a mere $50 billion turnover—why do you think those mega, mega American companies are going to co-operate with UK law, which does not technically and legally apply to them?

Sir Peter Fahy: I think, first, if Parliament passes that legislation it is a pretty strong indication of the will of the country and therefore there has to be a moral obligation upon them. Clearly, all the time we deal with different commercial organisations who sometimes make decisions as to whether to co-operate with policing and with law enforcement or not. We have to cope with that in our day-to-day business and I think it would be absolutely about, sometimes, levering public pressure onto some of those organisations, if necessary, to name and shame, to say that, you know, "We feel you should be cooperating and helping us in this

form of law enforcement". In the same way as we might choose to shame a car park operator if they are not taking sensible precautions.

Q1083 The Chairman: Do you mean shame companies like Google and Facebook?

Sir Peter Fahy: If we need to do that. If it was the sort of serious offending that the public feels very, very strongly about, then I think that we would absolutely need to do that.

Q1084 Lord Strasburger: We heard evidence in the previous session that that sort of heavy-handed approach was likely to diminish the voluntary co-operation you are currently getting.

Sir Peter Fahy: I think, normally, again, when you are talking to a car park operator or to a major supermarket or to a public house you try and do it through co-operation and, generally, that will work. But I think if you were faced with, as you say, one of these international organisations, which was failing to co-operate and which was not following the legislation, then I think clearly we would be talking to the media and to some of our local and national politicians to make them aware of that, and then clearly they may choose whether or not to apply pressure on them.

Q1085 The Chairman: Sir Peter, you said if the United Kingdom Government passes legislation we symbolically show to, say, companies in America we mean business. If Saudi Arabia passed the same sort of legislation, being one of the United States' major customers, would they not feel under a moral obligation to supply it all to Saudi Arabia or China or any other country that passes a similar law?

Sir Peter Fahy: It might well be, but I still think that, on the whole, the sort of issues we are dealing with here and the sort of investigations we are carrying out, there is a very high degree of public concern. I do not believe that some of these commercial companies could ignore that degree of public concern. Clearly, there are issues that, on the face of it, to international companies, may not look that important but which are perhaps leading to serious consequences in this country for individuals, and we know that the public and the media can be very concerned even about individual cases. If it came across, as I say, that a commercial organisation had made it more difficult for us to discover a perpetrator and that had led to a tragedy, then I do not think it would be terribly good for that particular organisation.

Q1086 The Chairman: Mr Davies, do you want to come in?

Peter Davies: I just wanted to add something. People have been very quick to identify implementation issues or enforcement issues around any of the proposed legislation. There is nothing wrong with that, but those issues in themselves are not sufficient reason not to bother to legislate, particularly in the face of a very clear operational requirement.

Q1087 Baroness Cohen of Pimlico: I would like to ask what you all think about the mutual legal assistance treaty process, which is of course the legal alternative—the undoubted, agreed, negotiated legal alternative. How well does that work?

Peter Davies: I think it works slowly. It certainly does not work in operational fast time, which is a proportion of the authorities that we require, and I really must hope that I have the opportunity to put a couple of cases to you that illustrate how direct and important some of this information is. It works with those countries with which we have a mutual legal assistance treaty, but not with those with which we do not, and my centre is quite often in the position of having to ask for help in the absence of any such treaty. Generally, we do quite well at getting it, but it is pretty random. I would not see the MLAT process as an alternative to the legislation as proposed.

Q1088 Michael Ellis: Chief Constable, I will come to you first of all. First of all, my condolences on the loss of two fine, brave, police officers earlier this year.

Lord Armstrong of Ilminster: Hear, hear.

Michael Ellis: That case I know is active, but there was some reference at the time, at least, in the media, and I think you have made some reference today, to issues within your force area of organised gang activity and that being a serious problem. Would you agree with that?

Sir Peter Fahy: Absolutely.

Q1089 Michael Ellis: Do you have any observations in that context about the value of communications data?

Sir Peter Fahy: I certainly think that, in terms of our current capability, communications data is absolutely vital to some of the successes that we have had, because it comes down to this issue of being able to try to prove associations. It is essentially that if you live in a nice area of Manchester and your house gets broken into and your car gets stolen, you are probably not aware that there is a connection there to organised crime, who are creating the market for that vehicle and probably put the offenders up to committing that crime. At the moment, communications data is absolutely enabling us to identify those sorts of associations.

Q1090 Michael Ellis: So you can prove an association with organised gangs in circumstances where otherwise you might not be able to do so and where such an association is not transparent.

Sir Peter Fahy: Absolutely, because of the way that they are using communications data at the moment. The situation is that when we arrest them and when we charge them they get disclosure through the criminal justice system, they become aware of our tactics, they go to prison, and they sit around all day and discuss, "How did the police capture us this time?" They are aware of the new technologies as really everybody is, but particularly every young person is, and, when they come out, they start exploiting those new technologies. We are starting to see that and that is our concern.

Q1091 Michael Ellis: What sorts of technologies are they starting to exploit?

Sir Peter Fahy: I do not want to go into too many specifics, because I am aware that they are probably listening to me now, but certainly it is essentially particularly some of the new platforms that are available, some of the gaming platforms, and some of the games systems.

Q1092 Michael Ellis: That is what I was going to ask you, about the gaming consoles and platforms. It might not be apparent immediately to everyone, but people can communicate with each other—I will not mention any trade names—from these very common games consoles.

Sir Peter Fahy: As you are playing the games and sometimes you are playing those games on the internet with other people, you can use that to communicate.

Q1093 Michael Ellis: Have you seen examples where some of these sophisticated criminal gangs are using those modes of communication?

Sir Peter Fahy: We have, yes.

Q1094 Michael Ellis: Would you therefore say that the legislation envisaged by this draft Bill is a vital operational requirement for you in moving forward to defeat these criminal enterprises?

Sir Peter Fahy: Yes, absolutely, I would. It is a vital operation. We are very concerned about the new capabilities that are developing. We are very, very concerned that we will lose some of the ability and some of the capability that we have at the moment.

Q1095 Michael Ellis: Chief Constable, has the law kept up so far with the criminal activities?

Sir Peter Fahy: At the moment, it is just about there, but clearly we see it fairly soon losing that. Of course there are issues, absolutely, about our own training, about making sure that we are exploring how new opportunities are covered by that legislation, about talking to the commissioners about that and how that will do so, and about how we create that capability within law enforcement. These are all challenges that we are facing, but absolutely we need the legislation to enable us to do that.

Q1096 Michael Ellis: We are at the status quo at the moment, but you would envisage even by the time Parliament takes to pass legislation we need to work to keep up with it.

Sir Peter Fahy: Absolutely. We are seeing this immediately. I was in one of my major investigation rooms this morning. We are seeing this now, so we are seriously concerned that in a short period of time we will start to lose that capability because, as I said, the criminals are very aware of this. They are aware of our tactics and capabilities.

David Stevenson: I just wanted to give you an example of how that has been put into practice. We had an organised crime gang that was using mobile telephony. They were using that to contact a logistics company where they had details of certain consignments. They had those transferred to a different address and made off with the goods. This was national and they did this on several occasions over a six-month period. We were able to identify the mobiles used, worked that the whole way through and eventually it led to very, very little, other than we identified the methodology and the company shut it down so they could not do it anymore.

They then transferred onto the internet, where they set up bogus accounts. They set up accounts that were very, very close to legitimate businesses. From those accounts they were able to generate email addresses that looked exactly the same, bar a hyphen, that came from these. So they then got these companies, unfortunately, to transfer these goods somewhere else where they made off with them.

Now, we were able to get the IP addresses from the domain name where this was set up. It was set up—they are very, very clever—using stolen credit cards, using wi-fi, using different bits and pieces that we were not able to trace, until eventually we were able to find out that the IP address that logged on to create that domain account initially led back to the leader of the organised crime gang's house.

So all we need is to keep the capabilities that we currently have, and I am sure you have been listening to the news today where LTE has landed. That is "long term evolution", which is 4G. Now, 4G offers data over the internet at very, very fast speeds. It is much, much cheaper than ordinary telephony. What we have at the minute is a situation where, if communication service providers are keeping this data for business purposes, we can get access to that. If they no longer have a business need to keep this data, if they offer an "all you can eat" tariff for everything, they will not need to keep any of this data, and this legislation is to try and protect what we currently have.

Peter Davies: I agree with what has been said. I just picked up that people might have the impression that everything is fine about the current arrangements. This is not to diminish the importance of future-proofing, and the arrival of 4G is a great example, but everything is not fine about what we currently have. If you are using high-volume data inquiries to investigate an organised crime group in relatively slow time, a 75% hit rate may be adequate. If one piece of communications data is the difference between life or death, or serious harm to a child or not, then leaving it to three out of four is not adequate. I would like to mention three cases very briefly that I think it is really important that I have the chance to mention, if I may. These are cases from within the last eight weeks in CEOP.

First, the good news: a contact between a child and a helpline service online, where the child indicated that they had self-harmed and were intending to commit suicide. Following normal procedure, this was passed on to CEOP as the agency that tries to reconcile the IP address to an individual. We did so in a very short space of time. We passed it on to the local police force in a very short space of time. They responded in a very short space of time and when they got into the address where we located this person, the child had already hanged himself, but was still breathing. Now, if there had been any delay in that process or if the child had been unlucky enough to be using one of the service providers that does not come up to the three out of four mark, that child would now be dead, and I do not think there is any level of tolerance or acceptance that that might have had a different outcome.

There are two other examples where we do not know what happened. I do not normally use these words, but I think it is important to convey this: there was somebody using a paedophilic chat room called "Child rape torture brutality". That is the name of the chat room. An individual had been on there once recently and once previously, and, quite simply, we were unable to identify this individual because the communications service provider does not record the IP subscriber information. I am sure you would expect me or any one of the 100,000-plus police officers, if we knew who was going onto this site, to do something to investigate and mitigate the risk they present to the public, but this was one of those occasions when we could not. I do not know who that person is, which is why I am not afraid to share that with you.

One more example, from this month: somebody offered online, for distribution, a number of indecent images of children, including files indicating the rape of a female four-year-old. We were unable to identify the suspect, because the comms service provider does not record the IP subscriber information and there were no other lines of inquiry.

Ladies and gents, I think it is really important to acknowledge that the communications data retention, accessibility and availability is the difference, in some of our cases, between children coming to serious harm or not, and I am grateful to have had the opportunity to convey those recent cases to you.

Q1097 The Chairman: In all of those cases, it is IP addresses that were the missing ingredient, not everything else in Clause 1.

Peter Davies: Yes.

Q1098 Michael Ellis: Mr Davies, if I may say so through you, Lord Chairman, you in child exploitation and your officers do a very difficult job and one that is very much appreciated. Thank you for enlightening us about those examples. I take it from that that you would wish to emphasise that it is not just a question of the status quo, retaining abilities that law enforcement currently have. We need to move in line with advances in criminal activities and therefore enact measures that will help law enforcement deal with these issues.

Peter Davies: Absolutely, and my point is that the status quo, while tolerable in most circumstances, I do not feel is tolerable in the circumstances I have described.

Q1099 Dr Huppert: Sir Peter, you were talking and following, I have to say, very nicely the Home Secretary's line about games and other online activities like that, and how legislation was needed because people talk on games. Can you tell me which bit of RIPA does not apply to that already?

Sir Peter Fahy: It is not about RIPA. It is, exactly as Mr Davies described, about the fact that the organisations that are providing this capability have retained the data, so that we can identify who the people are who using it.

Q1100 Dr Huppert: Are you saying that the whole issue about whether it is online games and the fact that people do all sorts of things like that is a complete red herring? It is about whether you have the IP address data.

Sir Peter Fahy: Yes, absolutely. It is about whether that provider has retained that data and we can get into it.

Q1101 Dr Huppert: So you would advise the Home Secretary to talk about IP data rather than online gaming as a particular issue.

Sir Peter Fahy: We are just trying to give—and I probably think she drew it from me rather than me draw it from her, but clearly we have been talking to the Home Office about what we are seeing in terms of the methods that criminals are using. We have used that as an example, but I would not want to limit it to that. What we are seeing, as I say, is a huge development of apps and of different offerings from different providers, and some of it feels certainly that it is only designed as a means of getting around law enforcement. Some of it is also to get around not being charged. There are services where essentially you can get a phone number and a means of communication that essentially means you are no longer paying a mobile phone bill. It is that sort of thing that we are concerned about, which is developing.

Q1102 Craig Whittaker: Can I just ask a question for absolute clarity? One would presume that because you know about these apps and you know about the gaming scenario, that if you need that information you can approach these companies and get the information going forward. The issue, I presume, is about what has happened; is that right?

Sir Peter Fahy: It is clearly whether that company chooses to retain that data.

Q1103 Craig Whittaker: But you can still request them going forward to retain that data for a period of time, so that they could help with your inquiry. I know it is not going to help in a life-and-death situation, but for serious crime, which is what you are talking about, it is about what has happened, rather than what is going on at present.

Sir Peter Fahy: Yes, that is right, but I would agree with what Mr Davies said. Clearly, even in terms of our current capabilities, there are a lot of frustrations, because again, if you are talking about mobile telephony, the criminals will do everything they can to make it more difficult to identify who has what phone. But that is a separate issue.

Q1104 Lord Strasburger: Mr Stevenson, can we go back to the example that you gave us, which was a very interesting one. Presumably, that was an ongoing investigation where you had identified suspects.

David Stevenson: Yes.

Q1105 Lord Strasburger: Surely intercept evidence would have given you everything you needed, and far more than you would get out of communications data.

David Stevenson: My knowledge of that is very, very limited. That is a completely different area and I would not be able to speak about it.

Q1106 Lord Strasburger: My understanding is that this is exactly the sort of case where you would go to intercept, with a warrant, and you would get all the information you want and more that way.

David Stevenson: Again, I am unable to speak about that specifically. However, if the Lord Chairman wants, certain evidence can be given in a written form.

Q1107 The Chairman: Yes, we will ask briefly on that, because it did strike me as well that probably going to the Secretary of State's warrant in Northern Ireland to get intercept evidence when you have known suspects may have been a route. It may have been used and you are not aware of it, in any case, at your rank, Mr Stevenson.

Sir Peter Fahy: We would have to say that the criteria for getting intercept from a Home Secretary's signature is extremely, extremely high and therefore we would not normally think about it in a case that involved the theft of property in this way.

Steve Higgins: I have just a brief point. The focus has been very much on serious and organised crime, and I completely understand that and support everything that has been said. There is another facet to this that may be worthy of note, which is the unwitting. A lot of these technologies are now used as a matter of fashion, rather than a deliberate attempt at subterfuge and I think that is a key point to bear in mind. In policing, clearly our primary focus is about saving life, followed by the prevention and detection of crime. The issue is that, certainly for the general public, a lot of their key concerns are about volume crime and in these areas where you have unwitting use of technology that does frustrate, that is a problem. To come back to the point that you made about the other alternatives that are open to us, clearly in those cases that would not be an option.

Q1108 The Chairman: DCI Higgins, a lot of these things you say may be fashion and there is a problem for the police in keeping up with it. We have had evidence from witnesses in the past who have said that a large part of this problem could be solved by better police training or better SPOC training, so they can know what they are asking for from the huge amount of extra information you now have available, much more than you had in 2000. Are the police fully trained to ask the right questions and to spot the evidence that may exist at the moment?

Steve Higgins: I think there are probably a number of questions sitting under that one, Lord Chairman, so I will perhaps try and address them in order.

Are the police equipped and do they have sufficient knowledge? In April 2010, we conducted a national training needs analysis to look at just this very issue; we identified a number of skills gaps, not just in relation to accredited SPOCS but also in relation to investigators and analysts, in particular. We have approached that over the last two years in a number of ways.

Specifically in relation to SPOCs, we introduced a programme to refresh the knowledge of every accredited SPOC in the country. That was in the form of a three-day course that was rolled out. We are currently looking at the accreditation of SPOCs and reviewing that, and looking to introduce a programme of continued professional development, applying a framework of information, so moving away from perhaps the old approach of a single course and then a number of ad hoc attendances at seminars, through to a more consistent national standard in that regard.

If I move on to investigators and analysts, again there was a significant gap that was identified in relation to this. The way that we have approached that is we introduced a

five-day course, which is the Core Skills in Communications Data course. That has now been rolled out, since October 2010, to over 5,000 police officers and staff. The follow-on from that is that we are now looking to embed that training within existing programmes of training that are rolled out to trainee detectives within the Professionalising Investigation Programme, which is a national programme run by the NPIA. In this way, the standard that we sought to bring detectives up to two years ago or a year ago, is now embedded within new-to-role training. We are looking now specifically at more specialised areas of training and so, in relation to analysts, we have just rolled out a six-day classroom-based course for specifically targeting analysts in the use and exploitation of communications data. We have also rolled out a specialist course for radio frequency technicians. We are currently looking at the possibility of rolling out dedicated training for a more limited number of detectives who are specifically involved in the more high-profile, complex and serious investigation of crime.

Q1109 The Chairman: What training do you do on advising SPOCs and officers on what is necessary and proportionate?

Steve Higgins: Clearly, that is a key part of their role, so part of their responsibility is to act as guardian and gatekeeper, as outlined in the Code of Practice. They are there to provide independent advice and judgment, if you like, both for the applicant and for the designated person who authorises the application process. They are taught very much to understand the difference between proportionality and necessity, and that a key part of the role is to scrutinise the applications that they receive. If I look at proportionality, it is about the level of intrusion into someone's privacy and whether that is balanced against the benefit to the investigation of that data. Necessity is about linking up the links between a mobile device, a crime scene and, potentially, a witness or suspect.

Q1110 The Chairman: We are aware of the filter arrangements—the RHID scheme—being developed. If, for the filter to work, there is a standardised Home Office-run set of questions or a program or format, do you then see less role for training SPOCs, if it is all going through a big centralised Home Office filter system?

Steve Higgins: No, I am afraid I do not, Lord Chairman. I think there is a basic requirement—and this has been reiterated by SPOCs such as Dave, who have been through the course and are very experienced now—for all SPOCs to understand the legislation, the application of that legislation within an investigative process, the network operations—so how networks operate and function—and also the data that is available to them. That is a basic requirement. I think the arrangements that you refer to that are set out within the Bill will help in certain circumstances potentially to reduce the burden on SPOCs. Again, it has been identified as a key challenge as more and more data becomes available and the thirst for data and information increases, not only to convict; investigation is about proving guilt and innocence, so it is about corroborating alibis as much as it is attempting to prosecute. I think the importance there is that potentially that will reduce the burden on the SPOC and the SPOC unit, but that will, in turn, free up their time, so that they can provide the advice and support that they are there to give to investigative teams

Q1111 Lord Strasburger: Do you have any training material on necessity and proportionality that you would be happy to share with the Committee?

Steve Higgins: I would be more than happy to share any training material or, indeed, if the Committee was minded, I am quite happy to facilitate a brief demonstration of a mixture of the training that is provided.

Lord Strasburger: I think we have missed the slot on that one, but the material would be useful.

Q1112 Dr Huppert: The training is clearly very important and the test around proportionality is really hard and it assumes that there is a reasonable way of judging that. You will know, presumably, that Derbyshire Chief Constable Mick Creedon, who runs Derbyshire Police and speaks on serious organised crime for ACPO, said about proportionality, "If I am driving on the motorway and I see someone on a phone and texting at 80 miles an hour, that, for me, would pass the test"—of proportionality—"immediately". Would you agree, in the absence of any other information, with the chief constable?

Steve Higgins: I think it would be inappropriate to comment with the absence of any other information. I think it is key to recognise that each case is considered on its merits.

Q1113 Dr Huppert: But he said given just that information that would pass the test. I realise that he is a slightly higher rank, but would you be training your SPOCs to reject an application from a chief constable? If not, are you not concerned that another chief constable may come in with something like that?

Steve Higgins: Absolutely, we do train our SPOCs to accept the position that they may well have to challenge upwards and that is part of their job; I think that is accepted.

Q1114 Dr Huppert: So you train your SPOCs that if they got a request like that they would say it was or was not proportionate.

Steve Higgins: As I say, I am not going to be drawn on a specific case without further information.

Sir Peter Fahy: I would be expecting them to ask, again, what the context is, whether there was a problem with fatalities on that particular stretch of motorway, or whether there were other circumstances.

Dr Huppert: And if there were no other circumstances?

Sir Peter Fahy: Again, I think what we are showing is that—

Q1115 The Chairman: We are getting a bit hypothetical now and into chief inspectors challenging chief constables, but Mr Davies wanted to comment.

Peter Davies: Which, if I may say so, in the context of RIPA, they are welcome to do and those are part of the rules. I know you know what I am going to say. I do not recall Mr Creedon saying that. I know it was attributed to him following a press conference, which I also spoke at. I do not remember him saying that at the time.

Following the last Committee appearance, I checked with him whether he had said that, because I must admit I would have been mildly surprised if he had. He said my recollection of what he said was accurate, which was that if you are investigating a fatal road traffic collision on a motorway, it is of evidential relevance whether somebody may have distracted themselves at the time of being involved in the collision by, for example, making a telephone call or texting. I think that would be proportionate. I think that is what I heard him say at the time and that is what he recalls having said subsequently.

Q1116 The Chairman: I have a completely different recollection, because I sat there at the time as well, but we will not debate that today and we will probably not be using it in our report.

Alan Lyon: I think it may be important at this juncture just to highlight the issue that not only is it important to train our SPOCs sufficiently, but also it would be helpful, I think, for the Committee to understand just where they are located and their relationship to their colleagues. They are very much separated from the investigative team and they work in a very confidential environment. They are vetted to an enhanced level, and access and control

to those members of staff working in that suite is very strictly controlled. So they do take their role as gatekeepers and challengers of senior officers, where it is appropriate, very, very seriously. I, as the senior responsible officer, do support them in that. It is a very, very important and key role for which they are properly trained, as my colleague has just outlined, but that is also a continuous professional development programme of regular training attendance. Of course, we are still under the scrutiny of IOCA.

Q1117 The Chairman: That is okay. I think the Committee has seen sufficient evidence that we are reasonably assured that they are not just rubber-stamping the requests of their pals. We realise that. A final question from me on this is: would you put the SPOC system on a statutory footing on the face of the Bill, the same as the Authorising Officer?

Alan Lyon: I am not quite sure whether there is a need. We have talked about necessity and proportionality. I am not convinced there is a need at this stage to do that and to be specific, as in the Authorising Officer's role. For me, my experience of the SPOCs—the way that they fulfil their duties, the way that they protect a very sensitive tactic and do it in a very responsible manner—does not give me cause within Greater Manchester for the need to do that.

Q1118 The Chairman: There may not be a need. Do you think it would give public reassurance?

Alan Lyon: There are perhaps other ways of giving public reassurance. I think the inspection process, which is independent and separate from the police, may be an opportunity to develop some sort of public communication programme that can reassure the public that Greater Manchester Police treats this particular sensitive tactic with the utmost respect and we deal with it in a very lawful and transparent way.

Q1119 The Chairman: Could that inspection process be beefed up a little bit?

Alan Lyon: Again, the inspection process is at the discretion of the independent panel, the Interception Commissioner, and if there was any concern about our handling of such a tactic they would inspect us more rigorously and more frequently than they do. I do find that the IOCA process is robust. Incidentally, our inspection takes place on Monday. The inspectors will be with us for three days and they will explore a broad spectrum of our work, from serious organised down to divisional crime, level two criminality, that we investigate and apply the tactic to. So it is very robust and they will be speaking not only to the SPOCs, but also to investigators and applicants and every tier of the process.

Sir Peter Fahy: I personally think it would be of benefit if the public perhaps understood a bit more about how seriously we do take this issue. I have certainly seen it in counterterrorist cases where the view is seems to be that the police can go around tapping everybody's phone, which is clearly not the case. We have put a huge amount of care into this, there is a huge amount of recording of data and, yes, I think sometimes it is frustrating.

Q1120 Michael Ellis: There is a lot of misinformation.

Sir Peter Fahy: Absolutely. I think it is frustrating that the public and some of the commentators do not seem to understand. I regard it very, very seriously, because this is an important capability. If there is any concern whatsoever from the public that we are using this inappropriately, that would be a huge damage to policing and a huge damage to victims of crime. My people know that I treat this very, very seriously because it is a very, very valuable tactic and if there was any cause for public concern that this was being abused, as I say, it would be very damaging to the police service and, probably more importantly, very damaging to the investigation of crime and protection of victims.

Peter Davies: Notwithstanding what Sir Peter and Mr Lyon have just said, the only other thing I would comment is, having tracked this debate for quite some time, if we had the choice between a beefing-up, through legislation, of the existing process of authorisation, transparency and accountability, I would regard that as preferable to the replacement of it with something entirely different, which was one of the ideas in circulation at the time of the last Committee and prior to that.

Q1121 The Chairman: You used my phrase "beefing up"; what is the beef?

Peter Davies: I was using the term "beefing up" in, I think, the same way as you were trying to use it, which is enhancing a system that is already there to provide a greater level of transparency and accountability, if that is required.

Q1122 Lord Strasburger: We have received evidence that the Interception of Communications Commissioner or a new body should have a more public role in reassuring the public that communications data is being used responsibly. How often are external checks presently carried out and what does the checking consist of?

Sir Peter Fahy: I would certainly, from my point of view, as I have indicated, welcome absolutely more public reassurance. Clearly, what we would not want is that to get into the description of some of the tactics that are being used, but I think it will possibly be something we want to discuss with the police and crime commissioners when they are elected later next month. So, absolutely, as I say, I have some frustrations: I would like the degree of seriousness that we treat this area in possibly to be better reflected with the public. I think you have heard we have a very rigorous inspection regime. We treat that very seriously and, to some extent, of course that is monitored week by week, because again certain of the RIPA authorities have to go to the commissioners and, if they do not approve of them or think the ones that we have approved were inappropriate, they will tell us very rapidly. So there is already the inspection regime, but, as I say, there is almost the daily monitoring of authorities and RIPA authorities and feedback coming back as to, "We agreed with that one" or "We did not agree with that one".

Q1123 Lord Strasburger: The Interception of Communications Commissioner's report for 2011 showed that they had carried out 22 fewer inspections of police forces in that year than there were police forces. So I can deduce from that that 22 police forces did not get inspected that year and, presumably, then went two years without an inspection. How frequently is your force inspected?

Alan Lyon: It is at the discretion of the commissioner. We were last inspected in September 2010 and, again, at their discretion, they are now due to visit us in November 2012. And for me, when we debrief the report on their findings and, indeed, brief the chief, we look at their recommendations, we look at their advice. In fact, since their last inspection process we have streamlined some application processes, because they found us being too challenging to our applicants. We have taken that advice onboard and have worked together collaboratively to reduce the number of applications and streamline them when appropriate, and that is fully within the legislation and fully within their guidelines. I think the very fact that they are coming back from 2010 into 2012 indicates a degree of confidence and satisfaction in their findings during that inspection.

Q1124 Lord Strasburger: Sir Peter, I think you were saying that you would be comfortable if the inspections were at least annual, to give the public more reassurance. That is what I understood you to say.

Sir Peter Fahy: It is really about the way that that is communicated. Essentially, if there was an inspection every year, but the public were unaware, then it would not be serving a great deal. I think there is an issue about how we communicate to the public the seriousness with which we treat this area. As I say, at the moment, when there are particular community concerns perhaps about a particular investigation, and often it is in the counterterrorist world, I think we certainly, at that stage, feel that some of the public and even some people who appear to be well informed do not actually understand how seriously we take it. But I would come back to: there is almost a daily interaction and we have had a particular type of authority where essentially the commissioners did not agree with us, and we had a fairly open conversation about it, but at the end of the day that was their decision. So it is a constant relationship in terms of how seriously they take it.

Q1125 Lord Strasburger: Are there any other changes any of you would like to see to the existing system?

Steve Higgins: Perhaps something to add, looking at inspection regimes, but maybe something worth pointing out is that the process by which we apply communications data is subject to routine scrutiny, because it is all subject to the CPIA. There is a requirement upon us to disclose that process through the courts. I requested just a brief review through the Metropolitan Police prosecution support team and asked them whether they were aware of any adverse court decisions on the basis of an abuse or a breach of that process, and they were not aware of any.

Q1126 Lord Faulks: Sir Peter, we have an independent reviewer of terrorism legislation. Do I understand what you are saying is that you would really like the equivalent publicity and priority and prominence to be given to those—such as the Information Commissioner—who are monitoring what you do, so the public gets an idea that there is someone independent on the case and reassuring them?

Sir Peter Fahy: I would be very, very clear that policing has always benefited from greater transparency and accountability, and I would be very, very clear about that as long as there is nothing that, perhaps by slowing things down, makes things more difficult. What I think is always interesting as well is we inspect on the basis of almost whether we have abused this legislation. We are never really inspected on "Are you making best use of this legislation?" And to be fair, I have had some commissioners who have said to me, "We think you could do more of this. We do not think we are getting enough applications from your force"—it was from a different force that I was in.

I think we have made it clear that we are trying to keep up with the training requirement, but I think, as every organisation, when you see the way this capability is growing, we absolutely do have a challenge in terms of training our staff, making sure we recruit the right staff to absolutely understand the capability, understand the legislation if we are going to keep up to that. Therefore, absolutely independent people who can help put some challenge to that are important; for instance, we in Greater Manchester are talking to our universities about whether they can help us in this area around research and capability and those sorts of things. But the general point I would make, as I say, is that policing has never had anything to fear from greater accountability and transparency. If that reassures the public that we are using this properly and that enables us to use the capability to then protect victims of crime, that essentially has to be a win-win for everybody.

Q1127 The Chairman: Are you aware, Sir Peter, of any forces who may be employing, next to the SPOCs, people who may be called "computer geeks", who may not

Sir Peter Fahy: We are increasingly trying to do that. Part of my reflection almost is that I need to recruit a room full of 14-year-olds to do this sort of thing, but there is a serious point to this: certainly some of our forms of recruitment in the past are not going to help us to survive in this territory. That is one of the reasons why we are talking to universities about whether they have good people that they would like to lend us, in terms of some of their research internships and those sorts of things, so absolutely we understand better their capabilities.

Q1128 Baroness Cohen of Pimlico: I think some of us who visited the Metropolitan Police formed a very favourable impression of the whole SPOC process. I think what we are trying to address is whether there is a better way not of doing it, but of getting it known that this Bill could be deployed to use. That is why we are asking whether the system could be made legally enforceable, because that would be infinitely reassuring to quite a lot of the general public.

Sir Peter Fahy: As a Chief Constable and from ACPO, clearly we now have a lot of defined roles in policing in terms of all sort of high risk areas, like firearms, counterterrorism, and even the investigation of murders. For instance, you have to be a senior investigating officer to investigate a murder; you have to have a record of achievement, all those sorts of things. We do not specify that in legislation, but it is absolutely there as what we now call "approved professional practice", which will now be signed off by the new College of Policing. I think we recognise that there is a need to show the public that we are professionalising policing and that absolutely there are key roles that we treat very seriously and are common across all forces.

Really, overall, that is the way that we would like to approach that probably, rather than just picking out particular roles because, as I say, the public should be equally concerned that the people who, for instance, are in charge of firearms operations themselves are trained to a certain level and it is treated very seriously. I think there would be a difficulty if we started to define all those different roles in legislation. It is rather about saying we take all these things very seriously in high risk activity. It is now in the new strategic policing requirement, which again has been approved by Parliament, and, as I say, will then go into an accreditation scheme in the new college of policing.

Q1129 The Chairman: On the other hand, we do not want deep public concern and thousands and thousands of people worried about how you investigate murder, and we do not have specific legislation on that. We are facing specific legislation here on a technical area where there is deep, deep public concern at the moment.

Sir Peter Fahy: Yes, indeed, and I think, as I have said, anything that would perhaps reassure the public and that would increase that transparency and accountability, we would not argue about.

Q1130 Lord Armstrong of Ilminster: I wonder if you would see any merit in creating a team of highly experienced and trained what you might call "super-SPOCs", who could provide oversight and advice. I am not suggesting that the Met or Greater Manchester necessarily need it, but it might be useful across forces, particularly for those police forces that only have occasional access.

Sir Peter Fahy: We recognise that in organisations like the NPIA and the Metropolitan Police, and even in CEOP, there is already a foundation of expertise. And again, the idea is that as we develop particularly the College of Policing, we absolutely would

like to have the idea around SPOCs and that expertise about this area within there. To a degree, we have that at the moment. You saw that in the case in Wales; when we have a particularly complex search you can go to various experts around the country who will help you, as a police force, in carrying out that search. I think your suggestion is a good one: that, essentially, in this sort of area there should be a group of experts identified that a particular force would want to go to. I think I have also expressed the concern I have that we need to build this capability for law enforcement, and we will be talking to the Home Office about, in the new world of the National Crime Agency and the College of Policing and other developments, where we will, as a country, be developing that capability around our understanding of communications data and the way that crime is going onto the internet in general. I would identify that, as a country, we need to build that capability. But particularly, as I say, around that area of expertise—around SPOCs and this particular area—I would like to see that developed within the new College of Policing, as a community of good practice that an individual force could approach if they wanted advice about a particular issue.

Q1131 Lord Armstrong of Ilminster: I am encouraged by that answer, Sir Peter. I wonder if I could ask a more general question, which you may not want to answer; I do not know. There is a scheme whereby local authorities who are minded to use communications data for investigations can use the services of the National Anti-Fraud Network. They do not have to, but they can use experienced SPOCs in the National Anti-Fraud Network and the evidence we have received suggests that the experienced SPOCs in that network do a very good job. I wonder if you think that it might be sensible to widen that service, so that all the public authorities that use communications data only occasionally had to put their requests through a centralised SPOC service, so that we got the level of experience and training and common practices and standards in relation to necessity and proportionality.

Sir Peter Fahy: I think, in general, we would support that. I think our concern has been that obviously sometimes the reported use of this type of legislation by certain other authorities has created the danger of calling it into disrepute. I think that is a risk for us in law enforcement in general, if the public and the media feel that some of that legislation, which they believed was intended for more serious forms of crime, was used for activities that the public themselves would not see as serious. That greater national oversight of that is something we would welcome.

Q1132 Lord Armstrong of Ilminster: Mr Davies, do you want to add to that at all?

Peter Davies: I just want to endorse that. I think most police forces use this kind of authority process fairly frequently. Practice may not make perfect, but it makes far closer to perfect. If it used rarely, then there will not be the expertise, and provided that expertise is provided from somewhere, through a scheme such as the one you describe, that has to be better than leaving it to people getting to grips with these kinds of powers, so I endorse what Sir Peter says.

Q1133 The Chairman: On bringing things into disrepute, you and many other witnesses have said and the Home Office in public session last week, "What we really need are IP addresses and weblogs". You and others have said, "We are really interested in who, when and possibly from what location"; that is pretty narrow. We have had witnesses who have said, "If that is all the Government wants, it is totally unfair to designate this Bill as a snooper's charter. But if Clause 1 stands as it does at the moment, then it is fair to designate it as a snooper's charter." How concerned are you that we have possibly got a draft Bill, which has been brought into disrepute because the Home Office have phrased Clause 1 so widely that, theoretically, everything could be caught. There has been inadequate consultation on it

and yet, as we get further and further into our inquiry, it seems that what they want and what you want are much narrower things than Clause 1 designates. My question is: have the Home Office made a rod for their own back in making Clause 1 so wide, because it does not seem to be what you need?

Sir Peter Fahy: We were obviously very, very concerned about some of the initial publicity and some of the public debate about this proposed Bill and some of the earlier forms of this Bill. We felt some of that debate was very, very ill-informed and did not take into account the nature of crime as we see it, the nature of organised crime, and the reality of the tactics that the criminals are using. Of course, again, chief constables, on the whole, were wary about getting into that debate, because it was becoming party-political and we are very wary of getting into that space, particularly after certain experiences we have had in the past. Unfortunately, that created a lot of information that this is now playing into and it feels like a bit of a catch-up to try and get across how serious this is.

In terms of the way the Bill is formed, we have certainly tried to express that it is trying to get the balance about absolutely reassuring the public and getting the balance with civil liberties right, but on the other hand, trying to make it broad enough to capture what might be future developments, so that we do not have to keep on coming back to this area.

Peter Davies: I will skirt around some of the observations you might be inviting me to make about how the Bill was formed, and so on. I think where I find my limits is in expressing the operational requirement for this kind of data to be captured, accessible and available in quick time, when necessary, to a whole variety of agencies whose business it is to enforce the law and protect the public. Whether Clause 1 overextends what is necessary, and it may well, that has to be a judgment for legislators, in my view. I think there may be some aspects of what is included that are more essential than others, but here is the thing: we are not legislators. We are here to express an operational requirement for data. So I am not sure I can answer the fullness of that question, but we understand entirely the need for accountability. We understand the relationship between possibly future-proofing this legislation and creating too much freedom and flexibility. I do not regard myself as an expert on how to navigate that, frankly. What I can say most clearly is that we look to you and the legislators to navigate that on behalf of the public, so that the right balance between the need to protect the public from harm and protect the public's right to privacy is struck. I am not the person who will advise you how to do that.

Sir Peter Fahy: The only other observation I would make from my experience is, overall, what has benefited this country and law enforcement is that we have been given the capability to use certain powers and certain capabilities that are sometimes denied in other countries. However, what has controlled that has been the level of oversight and inspection and regulation around that and the attitude that the courts take towards that. I personally think that is the right balance. You go to other countries where, for instance, there is no CCTV and the public would not trust the police with CCTV, whereas I think in this country we have that facility, it is there available for the public, but we treat it very seriously and control it very seriously. For me, that is the right balance. That is why, we would say, we would absolutely welcome any form of oversight or inspection if that reassures the public. That reassures them that the police are being properly overseen and regulated and then, as I have said, the victims of crime and those who may be victims of crime are getting the protection. I think the worst of all worlds is when society does not trust the police and does not give them the powers and capabilities, and it is the victims of crime who then lose out, and you do see that in some countries.

Q1134 Michael Ellis: Further to the point you made—I am not going to invite you to make politically loaded remarks; far from it—would you say that the media coverage has, in

places, certainly in the early stages of this matter, been a travesty of the truth. Certainly regarding talk of the Home Secretary being able to read people's shopping lists and the content of email, a lot of that was grossly misinformed. That is not a political point; that is simply an accurate reflection of the difference between what the draft Bill says and what was being reported. Would you agree, Sir Peter?

Sir Peter Fahy: I would agree with that and, obviously, I do see it from a certain point of view, as somebody who sees the consequences of serious and organised crime in communities and the way that blights the lives of people and destroys the aspirations of young people. I have that particular view of it, and in some of the comments I just did not recognise that people saw the reality of what it is that we are dealing with and the threat that it poses. I would also say that another break we have is the resources one. I do not have the resources to go on fishing expeditions through people's shopping lists. Every day, we have to look very, very carefully at a huge number of threats and consider where to concentrate resources, and some of the capability we have talked about is very expensive. I was looking at one investigation this morning that has cost us £30,000 just in communications data. So there are breaks in the system as well, but the situation we are in is that we have to look at the highest threats—we are often looking at people who already have pretty long criminal records—and try to deploy the tactic against them. We just do not have the capability or resources to go into these sorts of fishing expeditions that were described.

The Chairman: Okay, I think we get the message.

Q1135 Lord Armstrong of Ilminster: I just wanted to come back to the question of what they call future-proofing. We have a Bill and Clause 1, which endeavours to future-proof by throwing its net very, very wide. That has alarmed people, as we have heard. Insofar as it is an attempt to future-proof, it is a very difficult thing to do in any other way because we do not know what the future is going to be, so the only way you can proof against the future is by these very general provisions. The alternative is something more limited now, to deal with today's problems, and some kind of legislation in the future as new problems emerge. You will probably know as well as we do that there are great pressures on the legislative timetable. It is not easy to get legislation on such a subject frequently or quickly, and I wonder if you have any comments on that dilemma, because I think it is one of the dilemmas we face.

Sir Peter Fahy: I would totally agree with you. It seems to us, when you look at things like the potential development of 4G and other capabilities, that it is really impossible for legislation to keep up with that. Therefore, I would say that the alternative of the way you then operate the oversight regimes, the inspection regimes, the regulations that the Home Secretary may make to control this form of activity, and the way that the courts then view that, is a much better safeguard than trying to go through the legislative timetable to catch up. That, for me, is the right way to try and get the balance, but, as Mr Davies said, we are not experts on this. I think the concern absolutely, in lots of areas we see, is just the way that technology and societal attitudes are changing, which is very, very rapidly. For legislation and some of our processes to keep up with that is becoming more and more of a challenge.

Q1136 Lord Jones: The Lord Chairman made his remarks about Clause 1 just now, really a summation of a predicament we face with the draft Bill. Should we presume that in the private councils of ACPO there have been debates—lengthy debates, concerned debates? Does ACPO really get its teeth into the issues before it presents itself publicly?

Sir Peter Fahy: Absolutely. We have had a lot of discussion about this particular issue and, as I say, some really serious concern and worry about, essentially, what we are going to do in the future, if we lose some of the capabilities that we have at the moment,

because we have become so reliant on them. Things like interrogation, which perhaps worked 30 years ago, are no longer the tactics that we use.

Q1137 The Chairman: Let us be clear: you are not calling for them to be brought back.

Sir Peter Fahy: Indeed; I have been around too long. It is about having to get absolutely hard evidence from technology. But obviously there is a lot of angst at the moment about the level of public confidence and about questions of police integrity, and we treat that very, very seriously. And obviously there has been a lot of debate as well about, when issues become party-political—and there is an operational policing issue in there—how chief constables intervene to get the point across. We do treat that very seriously, because I think most of us think it is incredibly important that policing stays out of party politics.

The Chairman: I assure you I shall water-board Lord Jones later on.

Peter Davies: I would just like to offer a thought about Lord Armstrong's question. I do not think the basic principles of what communications data should deliver change. They are about subscriber information, service use information, and traffic data. What changes is where you might look for those pieces of data in a changing technological world, where people are far more adept and use social networking, for example, or gaming technology as their chosen means of communication. Those are the things that change. The principle of what we are looking for is exactly the same. Although some police habits have changed, as we have noticed over the last 30 years, looking for that kind of data, whether it is on a landline telephone or in the technology of five years' time, is what this is about. If it is possible to frame some legislation that enables law enforcement to carry on doing that, whatever the technological means by which that data may be found, that is what I think would be in the best interests of protecting the public.

Q1138 The Chairman: So we can put the principles into a Bill, which we amend every 10 years, like RIPA. If we were to be able to recommend to the Home Office, and if the Home Office were to be able to find machinery whereby the technical bits of where it can be found could be amended by order every year, by the Minister and through parliamentary scrutiny, you would be happier then that Clause 1 was not so wide-ranging.

Peter Davies: I would be happy enough. I keep repeating myself. I am not a legislator. I am not an expert on framing legislation, but I can tell you what the operational requirement is: it is as I have articulated. The best way of enabling people whose concerns are the protection of the public to access that communications data when they need it, in a proportionate, lawful, accountable and safe way, is what we are looking for. What you have just described does not sound like the worst of the options, by any means.

Q1139 Dr Huppert: Mr Ellis and I do not always agree on everything to do with this issue, but there is one thing I just wanted to agree on, which is that some of the media coverage in this area has not been very accurate. There is a risk about overstating what it will do, but also understating it. There was an article in the *Sun* at the beginning of this that said, "Only suspected terrorists, paedophiles or serious criminals will be investigated". Presumably you would not want to see inaccurate statements like that made when it would be used far wider. Is that correct?

Sir Peter Fahy: Yes, absolutely.

Q1140 Dr Huppert: That was the Home Secretary's article, so I hope we will hear from her tomorrow how she would correct it.

Sir Peter Fahy: There has obviously been some debate as well recently about the growing workload we are getting from investigating harassment on things like Facebook and some people seeing that as fairly low level. On the other hand, if a young person, God forbid, commits suicide because of bullying and harassment, the coroner may well have something fairly direct to say to the police force, such as, "Did you do everything to try and investigate that?" So I think that shows that these are serious issues, and that is why it has been difficult for policing overall and legislators to frame what is serious crime. Because often it is a bit like the guy texting on the motorway: it only becomes really serious when you see the consequence of whether somebody died as a result. That is part of the complication in this area, but as Peter and Mr Davies have shown, activities on the internet—that form of communication, the ability to commit crime on the internet, whether it is stealing goods and getting them delivered to bogus addresses or some of the other activity—is clearly an increasing part of our work.

The Chairman: Thank you very much. We have had a long but very worthwhile session. We are very grateful to all of you for coming here today. Thank you all very much. Your evidence has helped the Committee again slowly to claw its way towards a possible solution, or a possible report for the Home Office to come up with a solution. Thank you very much.