Evidence heard in Public Questions 127 - 220

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.
Q128 Dr Huppert: Can I start off by understanding how things operate under the existing laws? Can each of you say briefly how much communications data you currently use; how many requests you made in the last year, and to how many people did that apply; what were the purposes; and how many cases were successfully prosecuted or concluded?

Peter Davies: I cannot give you all that data. I am happy to supply it in writing later on. As a general overview, we make roughly 3,500 applications per year. A proportion of those are unsuccessful. We are slightly unlike some of my colleagues represented here, in that we do not then make arrests, for example. We pass high-quality intelligence on to others, including law enforcement and community and children’s services, so they can make safeguarding interventions or arrests. That is a picture of the volume. Something that slightly
distinguishes us is that the vast majority of those are communications related to online activity, so ours is a slightly different picture.

**Trevor Pearce:** Our focus is on serious organised crime. About 95% of my investigations will have some kind of communications data attached to them. For example, in April and May, of 13 cases prosecuted by the Crown Prosecution Service on our behalf, 12 had communications data fundamentally at the centre of them. In relation to the specific numbers, we are happy to follow up in communication.

**Donald Toon:** In 2011, we had 5,000 applications and 15,270 individual items of data. To give an indication of the impact, that is directly related to about £850 million of protected revenue in a significant number of cases.

**Q129 Dr Huppert:** In one year.

**Donald Toon:** In one year.

**Cressida Dick:** The Metropolitan Police have responsibility for a large proportion of serious crime, organised crime, counterterrorism and other forms of crime, so we use this in preventing and detecting crime. We also use it hugely in terms of saving people’s lives where there is an imminent threat to their lives. If I take the example of terrorism, we are the agency that, with the Crown Prosecution Service, brings evidence to court, so we present this data in evidential form as well. I cannot give you the exact figures, but we are by far the biggest police service and have much the biggest use of communications data.

**Q130 Dr Huppert:** But you would be able to send us the figures on the people, cases and requests.

**Cressida Dick:** I will certainly attempt to send you the figures you are looking for.

**Gary Beattidge:** In my two force areas, last year there were 10,107 applications, of which at the point of first contact 2,577—25.49%—were declined as not meeting the standard by our single point of contact. A further 112 were later declined by the dedicated person who reviewed these incidents. We have recently conducted a national two-week survey in respect of the number of applications, and I can provide that in written form to the Committee, should that be required.

**Q131 Dr Huppert:** I look forward to seeing more of that data. You clearly make considerable use of communications data at the moment, although I am slightly concerned about the 25% that are declined. What is not clear is the data that currently you cannot get. The Home Secretary has spoken about Facebook and Google. As I understand it, Facebook and Google do comply with a number of requests. What is it that you cannot get from them at the moment?

**Cressida Dick:** I am not technically qualified to tell you that. What I can say is that when I sit down with my senior investigating officers, both in counterterrorism and serious crime, they say they all have experience of not being able to get the data they would like, and they are feeling that increasingly.

**Q132 Dr Huppert:** But you do not know what sort of data it is. If Google said they would provide you with anything you asked for, you could not tell them what you wanted.

**Cressida Dick:** I am never myself an applicant. When we apply we are always very specific as to what we are looking for. There is an increasing amount that is either impossible or difficult to get.

**Q133 Dr Huppert:** Can you tell us what it is that is missing? We are trying to understand what gap needs to be closed so we can work out how to close it.
Cressida Dick: It would be difficult, for reasons you would understand, to be hugely specific about the precise type of data, or indeed the companies in some cases, because that is something that we, sitting here, do not want to tell all the criminals right now.

Q134 Lord Armstrong of Ilminster: Is it because the information is not available or because it is withheld by the service providers?
Cressida Dick: My understanding is that it is more often not available, and increasingly so. Occasionally, it is also withheld.

Q135 Dr Huppert: I think that both Mr Beautridge and Mr Davies want to comment.
Gary Beautridge: In some regards we do not know what we do not know. There is, however, a lot of information being requested through our own single points of contact that we know is not available. To open that up publicly would expose some vulnerabilities within the service. We would very much like to take the opportunity to write in on that specific point, which would illustrate the type of information we do not have access to.

Q136 Dr Huppert: I think that would be very helpful.
Peter Davies: I would like to echo that. There are two points. One is that there are certain types of data not currently available through any legislation that are gaps that we do not want to expose to the public, for reasons Commander Dick has highlighted. The other is that some providers are better, quicker and more comprehensive in providing the data on request than others, so some of this is occasionally about which provider you are going to ask and you have a different level of confidence in the likelihood of a reply.

Q137 Dr Huppert: Presumably, none of you has seen the draft order that would go with Clause 1 of the Bill. Do you have any way of knowing whether the data you are currently lacking would be acquired even under this legislation?
Cressida Dick: Speaking for myself, I believe this is absolutely fundamental. I would like to maintain our current capability. I am not technically qualified to describe how we would do that.

Q138 Dr Huppert: If there are people in your organisations who have the technical information that would be helpful to this Committee, we would appreciate seeing it.
Trevor Pearce: It may assist this Committee, as we have done with others, certainly in relation to SOCA because of its wider responsibilities around broader technical issues, if we offered the opportunity to come and take a briefing and watch this in action so we can provide more context to the answers that we are not able to give here.
Cressida Dick: We would all very much like that.

Q139 Dr Huppert: That might well be helpful. A number of the communication service providers overseas, which I understand from what the Home Office and Home Secretary have said are part of the issue, are based in the US. There are a number of other countries. There are mutual legal assistance treaties between us and the US, so presumably it would be possible to get data from them direct from source using the MLAT approach. Have any of you used that or had experience of doing that? You must do that in SOCA.
Trevor Pearce: It can be used through letters of request, but it is about the nature of what you can ask for. In some regards perhaps a specific piece of information can be obtained. More broadly, in terms of how you carry out an investigation when you are seeking a range of conspiratorial material, that is a greater challenge.
**Peter Davies**: I would agree with that. Where we go abroad, there are also issues in terms of duration of data retention, particularly in the online world. There may be some delay between the piece of data being sought and the request being submitted. There are MLATs and international letters of request, but there is a delay involved and that is where the time limit comes in. Some of the attrition in getting data back is due to the expiry of the time limits.

**Q140 Dr Huppert**: How long a delay? Does that just argue that the MLAT process could be made faster?

**Peter Davies**: I do not think it is necessarily all about that. I cannot give you an exact figure for the delay. What I can tell you is that if, say, we worked on the principle of retention for 12 months, there are some aspect of our investigations for which that would still not be long enough, and there is a delay in doing the international best process.

**Gary Beaumidge**: There is certainly an inconsistency of approach among different CSPs that are not located within this country. We approach them for information and evidence. Some supply it in the format required; others do not. At the moment, there is not a consistent approach to the provision of this information by overseas providers. I could also provide specific examples of that, should that be required.

**Q141 Craig Whittaker**: In what proportion of your overseas requests do you get no information at all? Is that a big problem for your organisations?

**Cressida Dick**: I would have to research that. With the Chairman’s permission, we would intend to give a written submission later, and we can put that into it.

**Peter Davies**: That would also be my response.

**Q142 Stephen Mosley**: We had quite a disruptive session yesterday because of the sceptics. A couple of them said, “We’re all carrying round in our pocket a tracking device”—one of these—and one of their concerns was the availability of passive information between a mobile phone and mobile base station. Would you want that sort of communications data within this Bill?

**Peter Davies**: For some time it has been possible, roughly or more precisely, to locate a mobile telephone through the use of communications data. A team I have led has used that as almost the sole means of detecting a serious double murder in one of my previous forces. I do not think that is a novelty. I do not quite understand the distinction between a smart phone, to which you are referring, and what has already been available for many years, which has helped protect the public and prosecute offenders in the past with less developed technology and mobile phones.

**Stephen Mosley**: Essentially, that communication would be classed as communications data as far as concern the law enforcement agencies.

**Donald Toon**: In terms of the identification of a location, certainly it would be classed as communications data.

**Q143 Lord Strasburger**: To seek clarification on MLAT, presumably that is two-way and gives the Americans the opportunity to make inquiries of whatever data we are retaining. Is that the case?

**Peter Davies**: The legal assistance process allows third-party states to make requests, if those requests are able to be made within the UK.

**Lord Strasburger**: If, as a consequence of this legislation, we expand the amount of data we are retaining, the Americans would potentially have access to that through MLAT.

**Trevor Pearce**: If the right consideration is in place.
Peter Davies: Anybody with whom we have a mutual assistance treaty would technically have access, but of course that would go through some kind of decision-making process in the UK.

Q144 The Chairman: ACC Bea utridge, you were able to give us detailed figures for your own force area, Kent. Would it be your understanding that every police force in the country would have exactly the same sort of data in the same detail?

Gary Bea utridge: They should have that type of information, and it should be capable of aggregation and submission to this Committee.

The Chairman: Do you submit it routinely to the Home Office?

Gary Bea utridge: In the annual inspection.

The Chairman: The Home Office should already have the aggregated figures for all the police forces in England and Wales.

Gary Bea utridge: I believe that should be the case.

The Chairman: That is very helpful.

Q145 Michael Ellis: The Government have emphasised the importance of communications data, particularly as regards law enforcement, security, intelligence agencies and the like, in apprehending criminals and protecting the public. Could each of you briefly say something about how important you perceive this data acquisition to be in your individual experiences? For example, Mr Toon, I think you said a few moments ago that as far as the Revenue is concerned, it was able to secure £850 million last year.

Donald Toon: That is correct. There is a range of data we obtain through communications data authorisations. 80% of what we obtain is section C data; essentially, it is a straightforward subscriber check. It enables us to identify individuals who are involved in a fraud and further the investigation. If you want specific examples, we had an operation that led to the conviction of Mr Kevin Burrage for alcohol excise diversion fraud.

Michael Ellis: How much was that worth?

Donald Toon: That particular fraud was £50 million a year. He was sentenced to 10 years in prison as the major perpetrator. He had been operating for a number of years, seeking to undermine the alcohol duty control system.

Michael Ellis: So, it is worth nearly £1 billion a year to the Revenue.

Donald Toon: Yes. One interesting point to go along with that is that the £850 million refers to the direct revenue loss prevented as a result of the investigations we carry out. In addition, often we use the results of the investigation to change our internal processes and procedures, or on occasion to advise Treasury and Ministers about potential changes to the law. That protects a significantly greater proportion of revenue.

Q146 Michael Ellis: Mr Davies, could you say something about how it has assisted child protection?

Peter Davies: You asked for personal experience. Can I offer just one example prior to child protection? The double murder inquiry I mentioned related to a retired couple shot dead in their home on the coast of Lincolnshire in August 2004 by, as it turned out, the pre-eminent organised crime group then operating in Nottinghamshire. Bluntly, without communications data relating to contacts between mobile phones it would not have been possible to detect that crime and lock up the people responsible. For all I know, they might still be operating in Nottinghamshire now had that not been possible.
Q147 Michael Ellis: That is one double murder in your experience.

Peter Davies: That is a double murder, but I think it illustrates how long this goes back in terms of being an issue. Bluntly, there were other people involved in the conspiracy whom it might have been possible to prosecute and convict, but who it was not possible to prosecute and convict because there was a data loss in that investigation.

To give a more recent example, a force for which I was responsible in operational terms commenced an inquiry into a small group of people operating a news group, facilitating the circulation of child abuse imagery on a worldwide basis with over 2,000 members. The force I was involved in led the investigation. In the course of that investigation, 132 children in the UK were safeguarded and protected, and nearly 200 suspects were arrested and a large number brought to justice. The four people at the heart of this news group operation, which was run for profit and, regrettably, enthusiasm, were convicted. Again, without access to communications data, those outcomes would not have been possible. With access to fully retained and accessible communications data, more people might have been brought to justice and more children safeguarded.

Michael Ellis: To be clear, you are saying that 132 children were safeguarded as a result of your access to communications data.

Peter Davies: Yes.

Michael Ellis: But you feel that, because of current gaps in your powers, some have not been safeguarded.

Peter Davies: Absolutely.

Q148 Michael Ellis: And some child sex offenders and paedophiles are getting away with it.

Peter Davies: Yes, and that is still the case today from my current perspective in CEOP. A third example: one of the things we do on a daily basis is help ChildLine in identifying children who contact them over the internet rather than by telephone. Frankly, it is inconceivable to me to envisage a society where law enforcement, or people like ChildLine, are denied the opportunity to identify children at risk of suicide, locate them and get the right thing done about them. That is more or less a daily occurrence in CEOP at the moment. We experience data loss there and with some of the serious offenders we are dealing with. There are more examples, but I need to be brief.

Trevor Pearce: If I may focus on two areas, in 240 cases last year we were able to prevent either threats to life or kidnaps; that is, attacks which would have taken place against members of the public. If those had taken place, we know that the cost of an average investigation into a murder is about £1.8 million, so, notwithstanding the issue of family and personal injury, there is a fiscal cost to this as well.

Secondly, 95% of our investigation will have some kind of communications data in place. Communications is one of the key enablers for organised criminals to operate. The range of communication capabilities they now have enables them to operate more conveniently for their purpose, and therefore that has to be available to us if we are to show the true extent of conspiracies. A significant number of our investigations go into the criminal justice system, and the process by which that communications data was acquired can be tested in court procedures, as well as the evidential interpretation of the material that is gathered.

Q149 Michael Ellis: As far as this point is concerned, you say there were 240 serious organised criminals—people involved in kidnapping and other very serious offences—in the last 12 months.

Trevor Pearce: No. Those were 240 potential threats to life averted through access to communications data, whether that is kidnapping or a significant contract to kill.
Michael Ellis: You put a cost of approaching £2 million on each investigation if you had not had the data.

Trevor Pearce: That would be right.

Michael Ellis: That is approximately £500 million saved by having the data.

Trevor Pearce: Yes.

Michael Ellis: Have you been restricted or obstructed because you are not able to access communications data at the moment in other investigations?

Trevor Pearce: As in previous answers, there are opportunities lost or not available, and we are happy to go into those in more detail.

Q150 Michael Ellis: Assistant Commissioner Dick, how do you feel about it from the perspective of the Metropolitan Police?

Cressida Dick: At the risk of echoing some of what my colleagues have said, from the point of view of the Metropolitan Police, if I take, as I did the other day, a completely random week, we would expect to have one kidnap, which is the sort of operation in which we are putting an enormous amount of resource, where communications data is absolutely fundamental. About five suicidal people will be found through communications data. We probably have an abduction—perhaps an honour-related abduction, or something like that—and other threats to life.

As to murders, speaking to my senior investigating officers, it is now extraordinarily rare to have a murder in London where communications data is not a fundamental part of the investigation. Indeed, if we look at Trident gun crime murders, which colleagues will probably be familiar with, in every single one communications data is fundamental to the investigation. You have very few witnesses; usually you have limited forensics; you are very limited in what you can do, but often there is a call from the offender to the suspect, or through another person, before the time. It is usually a group of people. They get together and communicate before and after. It is a vital part of our investigation.

As to robberies and rapes, it is very usual for phones to be stolen. The stranger rapist, on many occasions, will take the phone from the victim and within 24 hours we find the rapist.

If I turn to counterterrorism, you will be aware that every single major security service and police counterterrorism operation involves communications data. Looking at those that are very obviously in the public domain, in the 7/7 investigation communications data was very obviously extremely important. If you look at Seagram, which was the Glasgow attacks, we tracked them to Glasgow and found the bomb factory. For all of them we use communications data all the time, and the important thing is that the police use evidential communications data in these investigations.

Q151 Michael Ellis: This Bill seeks to redress a mischief. Both the Home Secretary and the Justice Secretary have indicated that there has been a degradation, which has been approximated at 25%, of the data that can be obtained by police and security services, so we are down to 75% of data. Are any of you able to share with us—those of you who have not already done so—any instance where this inability has impacted on the conduct of your investigation or prosecution of a case? Are there examples you can give of people who have not been prosecuted, despite the fact your investigating officers knew or believed they were involved in a ring or some other organised crime, because the evidence could not obtained?

Gary Beauchridge: I could certainly point to cases where there have been prosecutions in spite of not having earlier access to that data and we have only found out the activities of the individual in question significantly after the events have occurred. The most recent case under my command was the rape of an eight-year-old boy and 10-year-old girl. We could not
get the information we wanted and had to employ other techniques, which were ethically and technically extremely complex, expensive and lengthy, to bring the offender to justice because of the method of communication the offender was using, which was web-based communication. We have other cases, most recently one where three people were convicted of a triple murder, and the speed of the investigation was very much directed as a result of access to more conventional communications data. We could get on top of the case immediately and save hundreds, if not thousands, of man hours. We tracked the offenders from Coventry to Chatham in Kent where they set fire to a house and murdered three people. That is the opposite side of the spectrum to show how digital footprints are now key; they are not a “nice to have” but intrinsic to investigation and the core function of policing, which is looking after vulnerable people. That allows us to do that.

Q152 Michael Ellis: What are the categories of additional data that you would wish to be collected that providers either do not currently hold or you are not currently allowed to have access to under the legislation in situ that you believe would be necessary for investigatory purposes?

Gary Beauchridge: I think that would expose publicly some of the vulnerabilities of law enforcement. With your good grace, we would prefer to be able to submit written evidence in that regard.

Michael Ellis: Speaking for myself, I do not press you on that. As far as concerns this Bill, however, you are familiar with the terms of its clauses. Do you believe this Bill would redress some of the current gaps in policing as far as concern these issues?

Gary Beauchridge: I do, absolutely, yes.

Q153 The Chairman: Some of the critics of the Bill have said that often you are looking for a needle in a haystack, and if we now give you an extra few billion bits of evidence we have just made the haystack bigger. What is your response to that?

Gary Beauchridge: I would not agree with that position. Whatever we do, there is a proper intelligence and evidence base for making the application. Applications are made on the basis of necessity and proportionality. What should not be forgotten is that there is a real financial cost in getting this information, and a further cost if it needs to be presented evidentially. These matters are very carefully considered. The applications are made on the basis of intelligence, evidence and in furtherance of criminal investigations.

Peter Davies: The issue is partly to do with the assumptions that lie in the question. One of the key assumptions is that it is possible to make entirely speculative communications data requests and get them authorised. My experience is that that is simply not the case. More typically, one is confronted with a situation where, often after the fact, one wants to reconstruct a criminal network from one or two people.

Q154 The Chairman: You have a suspect in mind.

Peter Davies: Organised crime works through networks, and one has to reconstruct the whole network. The risk is that, if you settle for one part of the network and lock up only that person, the rest of the network is free to carry on offending. The concept that this is purely speculative is against all my experience and the procedures that currently apply.

Cressida Dick: If it is possible, I urge you to come and see one of our units, look at the application forms and talk to our staff. It is extremely precise and incredibly well supervised and scrutinised. It is not looking for a needle in a haystack on any occasion.

The Chairman: The Committee will consider seeing, either at SOCA or somewhere, how the data is inputted. We will probably want to study that in situ somewhere.
Q155 Lord Strasburger: Can we turn to the current authorisation arrangements under RIPA? The draft Bill has been criticised for not requiring public authorities, other than local authorities, to seek any independent authorisation to obtain communications data. Instead, a senior designated officer in the same organisation must authorise any request. How does this system presently operate in your organisations?

Trevor Pearce: The application is made to the SPOC who will advise before going on to the designated person, who can give authorisation, and then the CSPs. The notion is that, as well as making judgments about the legality and process around proportionality, necessity, etc, you need a degree of operational understanding, not in relation to the operation or activity taking place, where quite rightly there must be some degree of separation, but about the practicality of that as it fits in with an investigation or inquiry, and, certainly from the perspective of my organisation, the nature of the investigation.

Donald Toon: From my perspective, it depends. There are two levels of authorisation. In relation to the lower category of data, section C subscriber check data, we have 100 officers specifically trained to act as designated persons in relation to that data. The application goes from a case officer through a more senior verifying officer before it goes to the designated person for a decision, and then on to the CSP. I have three people in one specialist unit who are designated persons for all applications for the 20% of our requests that are for higher-level, more sensitive data.

Cressida Dick: It is very similar for us. We have two levels—the inspectors and superintendents—as the designated persons. The vast majority of our requests are in relation to subscriber checks. The officer goes through a supervisor. They seek advice from the single point of contact, who is a very highly trained person. They then put in their application. It goes to the designated person who comes back through the single point of contact. The designated person in the Met is almost never even in the same unit as the person who is making the application, and the people who are operating as the single point of contact are in a specific unit. They work together all the time, and they are also completely independent of the applicant.

Gary Beauchridge: From my perspective, there are very high levels of professionalism around this similar to Assistant Commissioner Dick’s summary. Last year there were 10,107 applications in Kent and Essex. These are made primarily either by detective constables or detective sergeants who are officers in the case. The applications go to a separate unit entirely divided from those officers and are assessed at the single point of contact. At that single point of contact, 2,577 were rejected. When they subsequently went through to the designated person, who is a superintendent—a very senior officer—a further 112 were rejected. Everything is looked at on the basis of necessity and proportionality. If it is for the investigation of crime and protection of vulnerable witnesses or people, we need to make sure that all the human rights considerations are properly considered and there is a process of justification that sits behind it. We would not want well-meaning individuals wading through a thicket of confusion around these issues. These are highly trained specialists who do this all the time and make proper decisions on the applications.

Peter Davies: I would like to make a more general point in answer to your question. I think I speak for all my colleagues, here and not here, in saying that we absolutely understand and respect the requirement to balance the occasional need for intrusion with a proper, transparent and accountable process to make sure the innocent are properly protected. In one or two of the conversations I have had on this issue previously I have sensed people have assumed that people would be better protected if there was an alternative means of providing authorisation. Can I invite you to take a very objective view about the realistic possibility of those alternatives, the cost of those alternatives and whether they are more likely to protect the innocent than the safeguards my colleagues have described? I echo that it is really
important, if it is at all possible for you, to go and see the process in action, because I think it brings it to life.

**Q156 Lord Strasburger:** Can you tell us how many convictions or disciplinary proceedings there have been for misuse of this system?

*Trevor Pearce:* In my organisation, none.

*Donald Toon:* We have had none in our organisation. Interestingly, we have issues about other forms of sensitive data, for example taxpayer data, where we dismiss staff regularly for breaches there, but I think the zero figure for us reflects the fact that this is a very closely controlled area with authorisation requirements before there is any access to the data itself.

*Gary Beautridge:* If we want the public to have confidence in the use of data like this by the police we have to take its guardianship very seriously, as we do. In respect of data breaches, the sanctions are extremely severe in Kent and Essex. We had one recent case, which I cannot talk about in detail because it is still going through the judicial process, where something linked to this type of issue has resulted in a criminal charge against a member of my organisation. That is currently going through the process.

**Q157 The Chairman:** ACC Beautridge, do I understand correctly that you are saying to the Committee that the civil liberties of the individuals and their privacy is better protected by a trained superintendent in the police force than by well-meaning individuals who may be magistrates?

*Gary Beautridge:* That is absolutely not what I said. I said that within the police service we do not want well-meaning amateurs dealing with these applications, which is why we train officers and designated persons to a very high level. Nationally, over the last two years, over 10,000 people have been trained in the use of communications data. That was absolutely not what I meant. I meant that we do not want an artisan approach within the service to deal with this very complex area of business.

**Q158 The Chairman:** I am glad of that clarification. I thought it was a general description of the magistracy. I want to be very careful here; I do not want to ask about a criminal case. In principle, would you be averse to having a criminal penalty in this Bill for officers of any organisation who break the rules?

*Gary Beautridge:* I cannot answer on behalf of ACPO in totality, because I have not discussed it with my colleagues. As a personal view, I would not be against that. This is a very serious issue.

*Trevor Pearce:* We are certainly used to it in other parts of the Regulation of Investigatory Powers Act, notably Part 1, so attaching criminality to communicating certain procedures or processes in place is already in the current legislation. We recognise it as absolutely vital in protecting those equities.

*Cressida Dick:* I can speak for the Commissioner and say we take any breach of any data incredibly seriously. We have had examples, not specifically to do with communications data but more generally, of data protection breaches and others, which we will pursue as far as we possibly can. Regularly, sadly, people end up in court for misconduct in public office, occasionally for computer misuse and data protection. Those are very powerful bits of legislation. If there was to be another aspect to this Bill, how on earth could we object to that? But we do already take this very seriously.

**Q159 The Chairman:** I appreciate there is a range of criminal sanctions in other legislation that could catch people here. I know that Parliament is always in danger of adding
a similar criminal penalty to every bit of legislation when it is already there. Do you think it would reassure the public if there was a specific criminal charge in this Bill?

Trevor Pearce: Yes.

Cressida Dick: I can see that.

Peter Davies: I have probably the dubious distinction of having personal experience of the consequences of these things not being done properly, not, I have to say, on my own part. In a force I worked in previously, processes were put in place that were below the standard expected by the Regulation of Investigatory Powers Act. The consequences were, first, that three expensive serious crime inquiries failed at the prosecution stage. The consequences for the officers involved, whether or not they were closely responsible for these problems or just associated with the inquiry, were very significant in terms of lengthy external misconduct inquiries and, for those responsible, sanctions. One of the other drivers for quality in this is the knowledge that a prosecution might fail because of lack of proper process being applied.

Q160 Michael Ellis: Each of you spoke of your own public authorities and how infrequent prosecutions or disciplinary action had tended to be for offences of this sort. Assistant Commissioner Dick, have you far more experience of dealing with misconduct in a public office for misuse of the police national computer, for example?

Cressida Dick: I regret to say that we do. Data misuse is a considerable risk for all police forces given the amount of personal data we have. Other systems are more vulnerable and easier to get access to than communications data.

Michael Ellis: Under the current legislation.

Cressida Dick: Yes.

Michael Ellis: You would say that the absence of prosecutions for communications data breaches, when juxtaposed with prosecutions for misuse of the police national computer, for example, is a reflection of the current security within the system as far as concerns communications data.

Cressida Dick: Absolutely. There is a very strong security regime around communications data.

Michael Ellis: Much stronger than for the police national computer, for example.

Cressida Dick: The nature of the police national computer is such that every single officer and some police staff, with some safeguards, can have access to it. The databases on which we keep this information are not the same at all.

Q161 Lord Faulks: I suppose that access to the police national computer gives you an idea of how these things can be misused. I appreciate what you have all said about the safeguards in existence. Do you think that such risk that it is, which you are protecting against, is a collateral use of material, or simply over-enthusiastic investigation?

Cressida Dick: When I was answering the last question, I was talking about deliberate leaking of information, potentially for money. The dangers of collateral intrusion are in the minds of all designated officers, and everybody who works with RIPA in all its aspects, all the time. We have to look constantly at the risk of collateral intrusion and how we will reduce and mitigate it. If there is a significant risk of collateral intrusion, which we regard as disproportionate and inappropriate, we will not authorise anything.

Q162 Lord Strasburger: There were 552,000 applications for data in the last year for which we have figures. I know that you collectively do not account for all of those but you probably account for a good number of them. I think that collectively you revealed to us one case of malpractice in applying for this data, if I am correct. There are probably only two possible explanations for that. The first is that your systems are incredibly watertight, and the
Gary Beautridge: I referred to one case within Kent and Essex. We could research if there have been other cases across the country. I think that to make the presumption on the effect of the one case in Kent and Essex and apply it to the national figures would be a dangerous thing to do. That would require more research.

Q163 Craig Whittaker: On the 552,000 applications, what proportion of those would you say are used in serious crime? We heard yesterday about applications also being used to chase up speeding fines, for example.

Gary Beautridge: I can answer some questions based on the recent national survey we have done over a two-week period. The results of that survey indicate that 72% of the data requests related to suspect inquiries, 18% to victims of crime, 2% to witnesses, and 8% to other issues, such as missing persons and vulnerable individuals. The results of that two-week survey could be made available to the Committee, should you require it.

Part of the remit of my day job is to tackle serious organised and economic crime within Kent and Essex. The recent national mapping of organised crime groups indicated there are over 8,000 nationally, and over 30,000 members of those groups. From my own experience over many years, an armed robber does not commit just armed robbery. People who are in this for financial gain take a blended approach to criminality for financial gain. If a burglary could release sufficient funds to somebody who commits armed robbery, they would commit that as well. When we are tackling organised crime groups, we will take them out in whatever way we can, as long as it is lawful and ethical. It is not just for the more substantive serious crimes; if we can take them out by other means, that is what we do. The use of communications data is intrinsic and absolutely vital to those investigations.

Q164 Craig Whittaker: I understand that, but my specific question was: what proportion of the information requests are for those serious crimes compared with non-serious crimes?

Gary Beautridge: We could certainly look to disaggregate that from the recent survey conducted over a two-week period nationally and supply that to the Committee.

Cressida Dick: For the Metropolitan Police, I can say that a large proportion is for serious crime. Obviously, there are different definitions of serious crime, but, however it is defined, they are what anybody would regard as serious crimes. You may have heard the commissioner quote the figure of 23%, or roughly a quarter of our requests, over the last five years being for murder. Within our murder and most serious crime investigations—I am sure colleagues to my right would say this as well—we tend often to make multiple requests. In counterterrorism we will make multiple requests for one particular case, so the less serious the smaller volume of requests in the case.

Q165 Craig Whittaker: What would be the impact on your organisations of a system that required you to seek prior judicial authorisation of all requests to access data?

Trevor Pearce: We would need to leave in place our internal processes, because that gives us the quality assurance and operational oversight that we require. There will be security, cost and bureaucratic considerations. The more significant consideration, particularly around some of our responsibilities in relation to threats to life, etc, is the ability to get this speedily on a 24/7 basis.

Donald Toon: I would certainly agree that we would have to retain the processes internally. The potential impact would be most crucially felt in those areas of investigation involving particularly large-scale organised fraud where the fraud moves very speedily. We
see a series of organisations who will, for example, change the communication devices they use almost on a daily basis.

**Q166 Craig Whittaker:** Where speed is of the essence, do you think it is possible to devise a system that could distinguish between urgent and non-urgent cases bearing in mind a warrant system, if that was introduced?

**Trevor Pearce:** You could design the system. The current system about direct and other forms of surveillance allows for urgency criteria. Of course, the answer is yes, and for all the right reasons we would want to work within those, but we would need to be reassured that the ability to act in situations of urgency and minimise bureaucracy in a time when we are clearly being asked to make significant efficiencies is important.

**Q167 Craig Whittaker:** If a system of prior authorisation was introduced, can you think of any particular permitted purpose for which authorisation should not apply?

**Cressida Dick:** I am not sure that is a question for us, with respect. I am quite comfortable that in policing it is likely that anybody, having listened to the evidence, would think the reasons we use it now are the ones that should probably be retained in the future.

**Q168 Craig Whittaker:** Does anybody have a different view? What would be your view on the creation of some form of half-way house system with a level of third-party control falling short of a full warrant system, either in terms of the process to be followed or the cases in which such control was required? Do you have any suggestions as to how such a system might work?

**Trevor Pearce:** The issues are security and safety of transmission, because this is, after all, data and we would need to be reassured that whatever the third party did and how they managed the process provided the same amount of scrutiny, information and assurance as you are seeking from us in terms of our current and future acquisition and usage. Security is a key issue, whether it is physical, technical or personal. That would need to be done, and the issue is availability and access, on which again we would want to be reassured.

**Gary Beautridge:** From my point of view, there are issues around what the capacity of that arrangement would look like and what the cost would be. To go back to what my colleagues have said previously, if it was at all feasible I would urge on you a visit to look at the levels of professionalism and rigour applied to existing processes that, in my view, work very well.

**Q169 Craig Whittaker:** Do you think there are any authorities at all that should be put outside a warrant system?

**Peter Davies:** To clarify the question, I think we might be saying that a warrant system would not be necessarily appropriate.

**Q170 The Chairman:** Hypothetically, if there was a warrant system, are there authorities or public bodies that should be exempt from it?

**Trevor Pearce:** It is difficult to conceive of why there should be a different approach if the considerations are the same.

**Q171 The Chairman:** Let me ask a slightly different question. Mr Pearce, you quoted 240 urgent cases involving threat to life and kidnapping. Everyone on the Committee would accept that in those cases there is an urgent need to get information and pursue those with the utmost speed and rigour, but would you draw a distinction between a basket of cases
like that and possibly tracking down paedophiles and perverts where sometimes you are years late on the case and there does not seem to be the urgency?

**Trevor Pearce:** There are two things: whether you have a reactive or proactive investigation. Significantly for us, where a large number of our investigations are drug-related, it is equally important to be able dynamically to go after numbers to enable us to identify and interdict a commodity of drugs before it hits the streets and our people become vulnerable.

**Q172 The Chairman:** Yes, but you draw a distinction between where there is a kidnap victim or threat to life and within 15 minutes you need mobile phone data and a case where 24 hours would suffice if you are chasing a known suspect.

**Peter Davies:** This is a distinction that is not uncommon in the exercise of a whole variety of different powers and procedures. There is the fast time and the slower time. Common sense dictates that there has to be the possibility of defining what is appropriate for fast time, for example a life at immediate risk, or loss of opportunity if it is not done very quickly. It is possible to make that distinction. It is analogous to other powers and processes, but I could not tell you exactly what it should look like in these circumstances.

**The Chairman:** I seem to have opened a can of worms.

**Q173 Stephen Mosley:** We have been talking about a warrant system before the request goes in. Would you have any thoughts on a notification process afterwards? If someone has had some sort of search done against their communications data, should there be a notification process in which they are told about it later, maybe with some sort of court process in there if, for some reason, you would not want them to know that because of an ongoing case?

**Peter Davies:** I am happy to follow up the previous point. I would not want you to assume that I think this is possibly the best way forward, but if you impose this kind of process the analogy is already there. Where people exercise powers in fast time there is a process of accountability to make sure the same scrutiny is applied, albeit retrospectively, because that is necessary. I think the analogy carries through to that. It would be possible to have some retrospective scrutiny and powers exercised in extreme circumstances of urgency.

**Cressida Dick:** At the risk of disagreeing with my colleague—I am sure we agree in some respects—there is a very high volume of cases involving long-term covert operations where we may or may not be successful in the first instance in bringing somebody to justice, and we would probably fight quite hard not to have to reveal the fact that they were targets, whether it is a counterterrorist or organised crime operation. I am no legal expert, but I think it would be a bit of a departure in our legal system.

**Trevor Pearce:** We are perhaps speaking at cross-purposes here. Peter has been referring to, in cases where authority has been granted, whether you notify some kind of body, like the Information Commissioner, that that has taken place. That happens now in relation to Police Act and RIPA authorities with the Information Commissioner’s Office.

The other point of your question was: is the member of the public subject to that entitled to have information made available to them somehow that a request had been made? I think that is more challenging. Investigations ebb and flow and you may well compromise an investigation against that individual or others, and that provides a risk. In terms of this proposed legislation, there is discussion about the role of something like the Investigatory Powers Tribunal. In other jurisdictions this does take place. Talking to colleagues in other jurisdictions, they find it operationally challenging.
Q174 Mr Brown: I would like us to take up the suggestion of a visit to see particularly how the authorisation system works in practice. It would be a good thing for us to do. How much of a practical possibility is it to obtain information from the system improperly, either for personal use or just out of curiosity? Can operators do that, or would they be immediately caught and prevented from doing it?

Cressida Dick: It is almost impossible. If you are the applicant, you have to apply with an intelligence case that relates to a real operation with real people and real data that you are seeking. The supervisor has to look at that and make sure that what you are asking for exists and is legitimate; likewise, the point of contact and the designated person. If you then ask whether the designated person or point of contact could do that, the answer is no, because there are different legs of the chair, if you like, all looking at each other and saying, “What is this case?”

Q175 Mr Brown: Is it a physical possibility to bypass that and get the information anyway?

Trevor Pearce: I would suggest not. As our IT systems get more sophisticated, you can put in algorithms which will identify anomalous behaviour. We share all our information assurance practices to make sure we are able to carry out those sorts of audits. There is a range of protections from the application and authorisation process itself, the separation of those roles, the reasons for acquisitions and the technical measures in place to check for anomalous behaviour.

Donald Toon: If you are asking whether it is possible theoretically, the answer must be yes, from my perspective, in relation to the designated persons who are the trained people authorising this. However, the systems in place would almost certainly ensure that if they did so they would do it once and would be caught immediately, because the cross-matching audit trail just would not exist.

Q176 Dr Huppert: To look again at the approach to warrants, we have looked at the issue of urgency versus non-urgency—I think we all accept there is a difference there—and the type of case. Clearly, a murder is very different from the speeding offences that Derbyshire’s chief constable seems to think count as serious enough to use this for. What about the option of separating it by the type of data? Some of you have indicated—I think it is true nationally—that most of the requests are for subscriber data, effectively reverse directory look-ups, which, to my mind at least, would be less intrusive than asking who somebody has rung over the last 12 months and exactly where they were when that happened. Would it be a possibility to have warrants only for the more intrusive types of request, for example, and to leave subscriber data requests under the current system? Would that satisfy many of your concerns?

Cressida Dick: Hypothetically, you could slice it different ways: urgency, certainly; seriousness, certainly; intrusiveness, certainly. You could try to slice it in all those ways, or in some combination of those. We believe that the disadvantages and disbenefits of that, given the strength of the current system, are very great and for us it would be difficult to justify going to that system, which would undoubtedly be a lot more costly and potentially burdensome.

The Chairman: This is fascinating. We are learning a lot, but we need to push on.

Q177 Lord Faulks: When I see the purposes contained in the draft Bill, they have their origins in RIPA. It is quite a long list. Criticism has been offered of the fact it is a long list and potentially puts the basis for obtaining information rather widely. I would like your comments as to whether you think it is too wide, and perhaps we can have assistance on
which of the permitted purposes currently are most often relied upon. I do not know whether you have the list of permitted purposes available.

**Donald Toon:** I can give you a very quick answer. 99.5% of our requests are for the prevention and detection of crime; 0.5% are for the assessment and collection of tax or duty. That 0.5% was 69 cases in 2011.

**Gary Beatridge:** From the point of view of policing, primarily, it is for the purpose of preventing and detecting crime, or preventing disorder; secondly, it is for the purpose in an emergency of preventing death or injury, or any damage to a person’s physical or mental health. I have not got the statistics, but I could provide them to you.

**Lord Faulks:** Are the many additions to those core permitted purposes used regularly? Is anybody aware of them being used?

**Trevor Pearce:** Not from my perspective. I am sure others in the Home Office may be able to provide advice on that.

**Q178 Lord Faulks:** Should there be any difference between the types of data you can request and the appropriate authorisation system? There has been some suggestion that maybe there should be a distinction between, say, serious crime and non-serious crime, however difficult that is to define. Does anybody have any views on that?

**Gary Beatridge:** It is a matter of trying to define serious crime, which is very subjective, and it would be difficult to ensure any clear and unambiguous interpretation. Working with the Communications Capabilities Directorate, we are introducing systems across the country to retrieve data in a more consistent format. I think that will help the contextual understanding of the overall situation and also reduce costs and the number of mistakes that may be being made at the moment, but it is subjective and ambiguous.

**Q179 Lord Jones:** Turning to misuse of data and monitoring, what level of monitoring and inspection occurs within your organisation to provide assurances to senior officers of the integrity of the SPOC process? How frequently has your organisation been inspected by the Interception of Communications Commissioner? How long did each inspection take, and what records were inspected on those occasions?

**Gary Beatridge:** The accredited officer role within our units is regarded as a gatekeeper. I have said previously that just over 20% of applications are declined by our single point of contact. Applications can be declined for a number of reasons: proportionality; collateral intrusion; and necessity. Once we have had a first look at the application, that goes on to a designated person. We also have refusals at that point. All of those applications are recorded in a system and are available for audits and inspection. We have an annual inspection by the Interception of Communications Commissioner. The last one concluded that the accredited officers were performing their guardianship roles and gatekeeper duties very effectively. In the last inspection for Kent and Essex, five recommendations were made. I could supply a copy of those recommendations to the Committee, should it think that would be useful.

**Q180 Lord Jones:** What lessons were learnt from the inspection, from the perspective of those who are giving evidence today?

**Trevor Pearce:** I do not have to hand the exact recommendations from our last inspection, but we are happy to share those with you and the action taken consequent on those. In addition to the range of management and supervisory responsibilities that go with this, as a non-departmental public body SOCA is also required to abide by the Cabinet Office guidelines in relation to information assurance, which itself is very rigorous. Having a senior information responsible officer within that process ensures that we look at the whole notion of
how we manage our information and the assurance of it in line with the best practices that we report on once a year. In addition to the Information Commissioner looking specifically at either interception or communications data issues, we have oversight in terms of how we manage information more broadly.

**Gary Beaunitridge:** Inspections are very intrusive. They last three days. All records are looked at; officers and staff are spoken to about the different roles and responsibilities in this process. There is a very full report and debriefing that results.

**Cressida Dick:** The Met also has the Interception Commissioner there at least once a year. They come for a week or more in a large team. They are very intrusive indeed; they spend a lot of time with the staff, but they also examine a very high volume of records. I think that in our case it is getting on for 1,000 records they have look at physically. They discuss their findings with us, including with an assistant commissioner, and make recommendations. Most recently, in our case they have identified some systems and administrative issues. They have also identified a couple of errors, which are useful to outline. Whenever we have an error that we ourselves find we must report it, and we do, to the Interception Commissioner. Then we must have an action plan about how we put that right. In the two errors they highlighted to us, we had sought more data than we had intended. The reason I give that example is that what the officers did was destroy the excess data straightaway. You might think that was the right thing to do, but it is not what the codes of practice say, but they were so concerned about it they destroyed the data and immediately told the Interception Commissioner.

**Lord Jones:** The impression given is that you demand integrity and very largely, as far as you know, you are getting it, and integrity in the operations of your given departments is a huge priority.

**Lord Armstrong of Ilminster:** I know there are difficulties about defining serious and non-serious crime, but I think there would be people outside who would suggest that there are some non-serious crimes for which access to communications data should not be allowed. We were told that 17% of police communications data requests were for non-serious crime. It would be interesting to know whether other witnesses would report similar figures. If people were worried about this, would it be possible to devise a system which excluded the use of communications data in relation to non-serious crime, for example bicycle theft or something like that? If one said that one would not use this intrusion for non-serious crime, would that be workable? What do you think about it? I think this applies particularly to the police.

**Cressida Dick:** It is potentially workable, but I would give two caveats. Sometimes a crime that is in a category that appears on the surface not to be so very serious—I think I am right in saying that burglary does not feature in many descriptions of serious crime—can be extremely impactive and very serious for the victim, and may be part of a series in which we fear what might happen next. One can imagine circumstances—indeed, in the Met we sometimes do give authority in relation to burglary—where the degree of harm is so very high that we regard it now as a very serious crime, even though it is not in that category. To take the driving example Dr Huppert referred to, in the Metropolitan Police it is not unusual for us, after a fatal collision, to make communications data inquiries. I am sure that nobody would normally refer to that as just a driving offence—if there was an offence—but it will feature in that category potentially, under “driving”. Most members of the public would expect, if there has been a fatal collision, that we will check to see that the driver was not texting or on the telephone at the point of collision.

**Peter Davies:** As to the difficulties of defining what is and is not serious, one way of doing that is to look at whether the offence is triable only at a magistrates’ court or Crown
Court. I will give you an example of why that is difficult. You may have heard of internet trolls who spend a large amount of their time inflicting serious psychological harm on people, for example through posting inappropriate messages or photographs on tribute sites to their recently deceased relatives. The appropriate offence for that is under the Malicious Communications Act, which is triable only at the magistrates’ court and is subject to time restrictions already. I think most people, certainly those affected by that kind of crime, would regard that as serious, and by its nature it is very difficult to investigate without communications data. I am not arguing for that to be included; I am merely observing how hard it is to draw a firm distinction between that which is serious and that which is not.

**Q182 Lord Jones:** Magistrates’ courts have been mentioned several times this morning. I think there are two: the district judge, the stipendiary, and the time-honoured three magistrates. Which would you prefer? Do you have a preference? Do you ask for one or the other?

**Peter Davies:** To clarify my answer, my point was more about the way the criminal law categorises malicious communications. I would not wish to express a personal preference, but colleagues may have a view.

**Q183 The Chairman:** Assistant Commissioner, you mentioned that in certain cases involving less serious crime one would need to check whether someone was texting or using a mobile phone on the motorway if there was a road accident. I confess an interest. Having been Police Minister, my admiration for the work of the police service is second to none. There are three constables in the Lords for whom I have tremendous respect: Condon, Dear and Stevens. Having said that, I am also cynical. Give the police a power for one thing and there is function creep; it gets extended to other areas. Within minutes of the Home Secretary at a press conference saying, “This is necessary for terrorism, paedophilia and serious crime”, Mr Mike Creedon said, “And of course if there’s someone on the motorway zooming along at 85 mph while texting, that is a threat to life, so we need to get that person, too.” Would you accept that it adds to the cynicism of some of those who are opposed to this Bill that, while we talk about terrorism, paedophilia and serious crime, there is a fear that if the police get this additional information it will be used to pursue other areas of crime that are not in that top-level category? It is an unfair question, but life is not fair.

**Peter Davies:** I was present at the press conference. My recollection of what Chief Constable Creedon said—he is not able to answer for himself here—was that it was in the context of using communications data to investigate fatal or serious road traffic collisions. That is an investigative staple. I appreciate and understand your point, but my understanding of what he was saying was more to do with the very serious consequences, which are to be prevented and avoided if at all possible, of people misusing communication devices while driving what are potentially lethal machines.

**Q184 The Chairman:** That was not quite my recollection, but let us not argue about it. What assurances can you give to prevent police function creep?

**Cressida Dick:** The assurance is how it is being used now, which we have discussed in some detail; the degree of seriousness with which we, as senior people, regard this; the systems we have in place; and the very proper safeguards in place, for example the commissioner coming to visit us. It is not for us to say what the police powers should or should not be and where they should be limited. I take your point entirely that intrusive powers should be used only when they are justified, and where that line should be drawn is a matter for Parliament. Rest assured, however, that, whatever we end up with, we will do our
level best to ensure there is no creep. We will invite inspection and will be happy to have safeguards.

**Q185 The Chairman:** You cannot say fairer than that. ACC Beautridge, I was under the impression that the statistics you gave for Kent already covered the breakdown of serious and less serious offences. Why is a two-week snapshot necessary in the country if you and all the other forces are providing this information?

**Gary Beautridge:** We wanted to make sure a national picture could be presented that looked at the number of applications, what they were for and different categories of the applications so we could derive meaning from all the data out there at the moment. There was a huge amount of data. The requirement for some analysis to derive some collective meaning is very important in the context of where we are, which was why we commissioned the study.

**The Chairman:** Thank you very much. We look forward to looking at the data from all the forces and the national snapshot, and we may come back to this. Assistant Commissioner and gentlemen, thank you very much. We have gone on longer than intended, but it has been very worthwhile.
Examination of Witnesses

Daniel Thornton, Head of Enforcement (Legal), FSA, Councillor Paul Bettison, Leader of Bracknell Forest Council, LGA Regulatory Champion and Member of the LGA Safer Communities Board, Gillian McGregor, Director of Operational Intelligence, UKBA, and Nick Tofiluk, Director of Regulatory Operations, Gambling Commission

Q186 The Chairman: Thank you very much for coming. Could you briefly state who you are for the record, starting with Mr Thornton?
Daniel Thornton: I am Daniel Thornton, Head of Legal in the Enforcement and Financial Crime Division of the Financial Services Authority.

Councillor Bettison: I am Councillor Paul Bettison. I am the lead member for regulatory services at the Local Government Association.

Gillian McGregor: I am Gillian McGregor, Director of Operational Intelligence in the UK Border Agency.

Nick Tofiluk: I am Nick Tofiluk, Director of Regulatory Operations at the Gambling Commission.

Q187 The Chairman: Thank you for coming. I am sorry we are starting slightly later than planned. We had a lot of information to collect in the last session. Can I begin by asking each of you some very brief starter questions? First, how often have you made requests for communications data in the past? Can each of you give us an answer, if you have it?

Daniel Thornton: As I understand it, we are the largest non-core authority in the use of communications data. I can give you the statistics for last year. We had 2,375 requests, of which about 65% related to subscriber data and about 35% related to more intrusive forms of communications data. Most of that was for the purposes of insider dealing criminal investigations, which is effectively an information crime, so it is all about the passage of information. That is why communications data form such an important part of our investigations.

Councillor Bettison: The Local Government Association is itself a membership body. Therefore, we never request communications data directly as we have no requirement so to do. Our individual member councils, however, can currently request communications data but only for the purpose of preventing or detecting crime or preventing disorder. These crimes are often targeted at the most vulnerable in our communities, and can include rogue traders, loan sharks, doorstep crime, antisocial behaviour, environmental crime, animal welfare issues and benefit fraud. The LGA does not itself collect data on the number of requests for communications data; we leave that to the Office of the Interception of Communications Commissioner. The annual report from the commissioner’s office indicates that all requests received from councils make up only 0.3% of all data requests. We believe this low figure shows that councils are exercising their powers in a proportionate way and requesting data only when absolutely necessary.

Gillian McGregor: In 2011, the Border Agency made 4,062 access requests. The Border Agency figures are included within the general law enforcement and security agency figures in the IOCCO reports. That is an increase on 2010 when we submitted 2,854 requests. We anticipate that this year the figure will be higher, which reflects the fact that the agency has taken on a much more central role in the investigation of serious crime in relation to immigration and border issues, such as drugs importation, facilitation and trafficking.

Nick Tofiluk: Because the numbers are so much smaller for us, being a relatively small organisation, we made 104 applications over the last three years, which averages 35 a
year. That resulted in 636 requests, of which 68% were for subscriber data, 24% for user data and 8% for traffic data.

Q188 The Chairman: I think each of you has told us what types of data you have tended to request.

Gillian McGregor: I do not think I did. To clarify it, our breakdown is that for subscriber data it is about 70%; for user data it is 5%; and for traffic data it is 25%.

Q189 The Chairman: Under which permitted purpose in RIPA have most of your requests been in the past?

Daniel Thornton: All of ours have been for preventing and detecting crime because they have been for the purposes of criminal investigations. To put a slight gloss on that, one of the new permitted purposes under this draft legislation is civil market abuse, which we also investigate, where we can impose a civil penalty. Those powers arise under the Financial Services and Markets Act and come from a European directive. The proposal in this legislation is that, instead of using that power, the power is streamlined under RIPA, or RIPA-type processes, to use the same sort of process. We adopt exactly the same processes using our FSMA powers as we do when using our RIPA powers. That is the breakdown of how we use it under the Act.

Councillor Bettison: All of ours are and will be for the prevention or detection of crime or preventing disorder.

Gillian McGregor: For the Border Agency, over 99% are for the purposes of preventing and detecting crime. A very small percentage is related to our statutory responsibilities for detention services. That is related to public safety and the maintenance of good order and discipline on the detention estate, but also prevention of escape and riots.

Nick Tofiluk: The prevention and detection of crime.

Q190 The Chairman: For what kinds of investigations, as far as you can tell us, do you use the communications data?

Daniel Thornton: Most of it relates to insider-trading investigations, principally about someone trading on the basis of insider information. There is often quite a long distance between the inside source and the person who is dealing. It is a form of organised crime. We see groups or rings of people who pass data between them, and therefore communications data is key to trying to work out the connections between the person who traded and where the inside source is. That is probably the principal means for which we use this data.

It also is important for market manipulation, for example people posting messages on bulletin boards to try to move a stock price and then trading on the back of that. That is one of the abuses we have seen. We also use it in the unauthorised business area; that is, people who are trading without authorisation, which is effectively a form of fraud, in that they are selling worthless investments to vulnerable consumers. We use that often to try to be sure who is calling the consumer. For example, a lot of these people will use false names, so often it is important to try to work out who is making the call. We have also used it in a similar investigation to track down from where a boiler room was operating. That is a group of criminals pressure-selling worthless investments. We used that to locate where they were operating from using internet data, for example, and executed a search warrant at the right premises.

Q191 The Chairman: Councillor Bettison, you gave us some examples. Could you rank them in order of the most used?
**Councillor Bettison**: Probably, these days most of the use relates to benefits fraud. We know that the Government’s message to benefit fraudsters is, “It’s not if we catch you but when.” Certainly, the use of these powers assists us to help the Government make good on their promise.

**The Chairman**: I presume that would be housing benefit at district rather than county council level.

**Councillor Bettison**: That is right. As Mr Thornton has said, it is often very much a question of tying in somebody who has given a false name, or no name, in a communication with someone. It is certainly in the realm of rogue traders as well. That is another very large use, bearing in mind how little we have to resort to it. But in those cases where we do have to resort to this sort of information, it is absolutely vital. I have a number of case histories, which I would be very happy to supply in writing if that would be useful, where conviction has been possible only by this type of information being available.

**Q192 The Chairman**: Would you be able to give us an assurance that some of the cases we have read about will no longer occur, such as check-ups being made on a parent as to where they live and the area in which their child goes to school, or whatever, which would seem to be an abuse?

**Councillor Bettison**: We are very conscious that, due in no small part to the activities of the national press, these very rare occasions make much bigger stories. The reality is that the public, therefore, need reassurance. That is why we are very happy indeed to continue to work under the extremely stringent regulation we have to abide by in order to access this information.

**Gillian McGregor**: In the Border Agency we use communications data for quite a wide range. If I was to rank them as you request, the most common use would be in relation to drug smuggling and the smuggling of prohibited items. That is a matter the agency is responsible for, and our customs colleagues have joined us. There is also facilitation and organised people smuggling; trafficking offences; bonded labour; vice, or vulnerable persons, including children. We also use communications data for other immigration offences, such as the use of forged and counterfeit documents and organised crime groups that might be involved in that sort of activity; and sham marriages and bogus colleges. There are a number of different things, but I would suggest that is the kind of ranking for which communications data would be used.

**Nick Tofiluk**: In the case of the commission, 79% of our applications are focused upon the offence of cheat. If I can put that in the context of something that is perhaps more recognisable—match-fixing and all that that entails—the commission is the lead for the intelligence function with colleagues from ACPO, sports governing bodies and betting operators to address this threat. That involves the corruption of betting markets and the facilitation of those prepared and able to manipulate sports events as well as betting events, predominantly online betting. It also involves the use of inside information, so there is a lot of similarity with my colleague from the FSA. 17% of our applications have been focused on those illegally supplying gaming machines, which is a very lucrative pastime, if I can call it that, or enterprise, to premises that are possibly unlicensed for such. It has not only a criminal aspect but also relates to the commission’s objective which is preventing harm to children, young persons and the vulnerable, which we think is very important. 4% relates to the unlicensed provision of gambling services. It is very much weighted in terms of match-fixing.

**Q193 The Chairman**: That is very helpful. My final starter question is: you have all pointed out that you are very low users. Why are you not using it a lot more? Gillian
McGregor, the Border Agency realises that it has a powerful tool here. You are going to double the intake, or the requests.

**Gillian McGregor:** We are making use of these powers daily, and our use is increasing. I gave the figure of 4,062 in 2011. We are projecting that for this year our figure will be in the region of 6,000, but we have to make sure that what we are requesting is proportionate and necessary. I think it reflects the balance between our central role as the law enforcement agency for this type of crime and the proportionality of what we are doing. We also have a very close relationship with other agencies, such as SOCA and ACPO, and on some occasions our investigations will be so serious that they will be elevated to those agencies.

**Q194 The Chairman:** Is the proportionality hurdle for you in some ways too high? Are you being judged against the same yardstick as the security services in dealing with terrorism or the police in people trafficking and paedophilia? Do you have to show the same level of proportionality in chasing illegal immigrants as our security services do in chasing terrorists?

**Gillian McGregor:** The elements of proportionality are similar, because lots of the investigations we are dealing with are on a par with some of the serious cases that the police and SOCA investigate. Our judgments on proportionality and necessity are similar.

**Q195 The Chairman:** Do any other witnesses wish to comment? Do you feel constrained? Would you like to use them a bit more if you could?

**Nick Tofiluk:** I echo that to a very great degree, and I think it follows on from the previous discussion about what we mean by “serious”. Towards the latter part of the previous session the word “harm” started to feature in the discussion. From the commission’s perspective, the licensing objective is very much focused on crime, and I would start to think about harm in terms of children, young persons and vulnerable people being exploited by gambling, and then fairness. For us, proportionality is a combination of the criminal impact and the wider harms. The commission has 200 staff in total, and therefore the ability to use the powers wisely in terms of resource efficiency, as well as our ability to use the data once we have got it, is constrained, but, as my colleague from UKBA has said, increasingly we work in collaboration on the more serious cases with police forces and HMRC, and because of the global nature of gaming and sport we are increasingly engaged in international collaborations.

**Q196 Lord Jones:** On the future use of communications data, none of the bodies on the panel here today is on the face of the draft Bill. This means that if you are to have access to the data you have to be added by order under the parliamentary process. Do you wish to have access to communications data in the future, and have you been given any assurances that you will be added?

**Daniel Thornton:** We are not on the face of the Bill, although one of its purposes, to combat civil market abuse, is an offence that only the Financial Services Authority can pursue, which could be said to be a slight contradiction. The reason for it being there is that it is in European law in the form of the market abuse directive regulation. We think we have a very strong case to have these powers. Whether that is on the face of the Bill or through a statutory instrument does not make any difference to us per se. We have to go through a process to get approval from the Home Office, but ultimately how that is done is really a matter for Parliament.

**Councillor Bettison:** Clause 11 of the draft Bill and the recent Protection of Freedoms Act provide councils with the power to continue to access communications data with the
approval of a magistrate. We believe this shows clear recognition by government of the importance of these powers for councils to protect their communities from crime. However, since the Bill was published the Home Office has advised the LGA that it is expected to make a business case for a specific order to ensure that councils can retain access to communications data. The changing stance, along with differing legal views about whether the order is required, has created significant confusion and concern about government intentions on the matter. It would be helpful to have a clear message from government to support the importance of councils retaining access to communications data to protect the most vulnerable parts of their communities from crime, and to acknowledge that councils are making good use of current powers in a wholly proportionate manner—witness the very small number of uses currently.

Lord Jones: Thank you for the information as to what the Home Office has said to you.

Gillian McGregor: The Border Agency is not on the face of the Bill, and that reflects the position in RIPA where our powers come from secondary legislation. Things have moved on for UKBA. We are recognised as a law enforcement partner with a very clear role. We want to retain access to communications data. Like my colleague Councillor Bettison, we have been asked to produce justification for that continued access. Similarly, the most important thing for us is to retain access to communications data. Whether that is through being named on the face of the Bill or through secondary legislation is possibly a secondary issue, but we want to retain access.

Q197 Mr Brown: Is it true for the FSA and the Gaming Commission that they have been asked to prepare for draft secondary legislation?
Daniel Thornton: We have been asked to provide data to the Home Office and present a business case as to why we should have access to communications data.
Mr Brown: Is that so for the Gaming Commission?
Nick Tofiluk: Yes.
Mr Brown: Why do we not seek a list of the organisations that have been asked to prepare for this eventuality? In other words, tell us something we do not know.

Q198 The Chairman: I agree entirely. We shall request that. What is your deadline for producing your business case? Are they all roughly the same?
Daniel Thornton: We are supposed to produce some data by 20 July.
Gillian McGregor: Yes; it is the same for us.
The Chairman: You are required to produce data, a business case and justification for having an order made in your favour.
Gillian McGregor: Yes.
The Chairman: You have to produce that evidence, data and justification by 20 July to the Home Office.
Daniel Thornton: That is right.
The Chairman: That is helpful.

Q199 Lord Jones: Can you tell us briefly what would be the implications for you if you did not have access to the data you want?
Daniel Thornton: That is somewhat speculative, but certainly with insider dealing many investigations would not get anywhere; it simply would not be detected. We would see suspicious dealing but would not be able to identify whether or not it was innocent. In most of our criminal insider-dealing prosecutions, communications data has formed a central part of the evidence. As it is about the passage of information, it is an offence that you prove through
circumstantial evidence. One of the most important parts of circumstantial evidence is the timeliness of communications and who was calling whom when. The insider calls somebody who then calls somebody else who then calls the dealer who immediately places a trade, for example. Showing that pattern of behaviour and calls is absolutely central to most of our prosecutions. If we did not have access to this data at all, it is likely that many crimes we currently prosecute we would not be able to prosecute at all.

Q200 Lord Armstrong of Ilminster: Do you think you ought to be on the face of the Bill? Would you prefer to be on the face of the Bill?
Daniel Thornton: I would prefer not to have to make a business case, if that is what it means.
Lord Armstrong of Ilminster: You might have to do that either way.
Daniel Thornton: Yes. As colleagues have said, for us the important thing is to have the power. Exactly how it is portrayed in legislation is really a matter for government and Parliament.
Councillor Bettison: I think that not to allow local authorities these powers would leave councils without the necessary tools to protect their residents and businesses and seriously undermine the Government’s message to benefit fraudsters: “It’s not if we catch you but when”. There have been a number of high-profile cases where benefit fraudsters have been identified, caught and dealt with. It is important that people understand that benefit fraud is not an easy way to win on the system, and to make sure they cannot.

Q201 Lord Jones: In your experience in local government, are there many benefit frauds? Is it very serious?
Councillor Bettison: That particular fraud is stealing from everyone, and if we are not careful it could become one of those victimless crimes, simply because we cannot identify everyone, because as taxpayers we are all victims of those crimes. It is very important that councils are seen to have the ability to find out if people are cheating the system and stop them doing so.

Q202 Lord Jones: Would your business plan include evidence that there are many cases?
Councillor Bettison: It would include the details such as we have of the magnitude of the problem, and also examples where the problem has been dealt with by the use of this data communications information.
Gillian McGregor: Similarly, if the Border Agency did not have access to this data it would seriously hamper our ability to investigate immigration and customs crime, particularly serious ones. The crimes we are dealing with are international, fast-moving and involve communication across borders, so we rely heavily on communications data. To give you a flavour, in 2011 we conducted 461 separate criminal investigations that involved access to communications data.
Nick Tofiluk: If I may return to the previous question, because I did not answer, we expect to be included on the list, and I would be extremely disappointed if we were not. I would be less bothered about whether that was by statutory instrument or on the face of the Bill. We were given powers for criminal prosecution under regulation, and I think that is totally consistent with what is expected of us as the core purpose of the Gambling Commission. If you think of our core purpose as regulating the gambling environment, a large proportion of it is now moving to a remote base. The global gross profit of remote gaming is increasing year on year.
The second part that makes the case for me in terms of our regulatory and associated functions, possibly policing functions, in that environment is that perhaps in two years’ time the licensing arrangements for those providing remote gambling to UK citizens will change. We will have to license those at the point of consumption, or what is provided to UK citizenry—presently we do not have to—which is likely, in my estimation, to increase five to six-fold the market in gross profit terms. Therefore, being able to understand and retrieve data from a remote environment, where the scale of gambling and the technology that supports it is fast-moving, is absolutely critical. In terms of our role in the lead for sports betting corruption and match-fixing, without the powers given to us under RIPA I do not think we would be able to perform that role.

Q203 Michael Ellis: Councillor Bettison, local authorities currently cannot request traffic data from service providers, whereas other bodies represented here can. The draft Bill replicates that limitation as far as local authorities are concerned, and further states that local authorities will be able to request only information that service providers continue to generate out of business need. This may be the result of a perception in some quarters that local authorities have been responsible for frivolous applications. I would like to give you the opportunity to say whether you think this limitation poses any problems for local authorities. Can you make a case for wider access?

Councillor Bettison: I am sure that, given due warning, we could make a case for wider access, but the Local Government Association itself does not collect data on actual use of data.

Michael Ellis: I accept that, but can you speak behalf of the local authorities you represent?

Councillor Bettison: As to whether or not we could use additional data, I am sure we could find cases where it would have been useful. Having said that, I am here today quite content with the powers that we believe are being offered to us and am not demanding greater powers. I would look for any assistance in dispelling any myth about our limited powers being the result of frivolous activities in the past, because I do not believe that to be the case.

Q204 Michael Ellis: I think I am right in saying that the other bodies represented here can request all types of communications data, including traffic data. For each of you who can, how often do you request traffic data, and in what kind of investigation is traffic data most useful?

Daniel Thornton: The first stage is often to get the subscriber data to work out who is calling whom, but traffic or use data is essential to work out the timing and length of telephone calls, for example. In some investigations, it has been important to work out where people are at particular times, or when they are logging on to, say, a secure internet site being used to deposit information. Our usage is probably between 30% to 40% per year for the more obtrusive forms, apart from subscriber data.

Gillian McGregor: The agency relies heavily on traffic data, so it forms about 25% of our data requests. I think the cases to which it is particularly relevant are trafficking, facilitation and smuggling offences where, like my colleagues, it is important to be able to be aware of movements, to know who has been talking to whom and how that is progressing. If it would help the Committee, we would be very happy to share examples of cases where traffic data has been particularly helpful in achieving a conviction.

Q205 Michael Ellis: Indeed. Could you give one brief example now?

Gillian McGregor: Yes, I could. We dealt with a major investigation into a serious organised crime group operating in Manchester, which was importing drugs. For that
particular investigation we used a mix of all the different types of communications data, including cell site data, through which we were able to track the movements of suspects, and, linking that with other information, we placed them in a position where we understood they were people operating the organised crime group. To give you the scale of the operation, it involved class A drugs—heroin—of a total weight of 175 kilograms with a street value of £13.5 million. The two main members of the organised crime group were sentenced respectively to 11 and nine years in prison, so traffic data was very important in that particular case.

Q206 Michael Ellis: Is it important to the Gambling Commission?

Nick Tofiluk: Very, and in almost exactly the same circumstances as my colleague from the FSA described. What we are trying to do is prove connectivity between facilitators who can influence sporting events, not just the result but incidents within them, and the placing of bets and communication between those people who are connected in that type of manipulation of the market.

Michael Ellis: Is it right that those of you who can utilise traffic data at the moment feel you need it, and you would be at a serious disadvantage if you were restricted in the same way local authorities currently are?

Daniel Thornton: Yes.

Gillian McGregor: Yes.

Q207 Michael Ellis: What percentage of communications data do you feel you need for your own investigations that is no longer available? We have heard about a degradation from 95% to 100% many years ago to 75%. Can you say something about how lack of this data has affected your investigations? Do you agree there is no longer as much access to data, for whatever reasons, as there used to be?

Daniel Thornton: It is very difficult to say. In our investigations we get quite close to the 12-month time limit because of their complexity. It is rather like an onion; you are peeling layer after layer to work out the connections, and by the time you get to where you want to be you are hitting the end of the period for which we know telecoms companies keep material. That is a definite limitation. What we do not know is the extent to which more sophisticated means of undetectable communication are being used at the moment. In our investigations we are seeing more sophisticated techniques being used, for example pay-as-you-go mobile phones but also self-destruct USB sticks to store sensitive data, which are passed between people, and the use of secure internet sites as a way of passing information. The people we are tracking are becoming more sophisticated in their techniques.

Michael Ellis: Self-destruct USB sticks.

Daniel Thornton: These are where you have hardware encryption, so if you enter the wrong password three times it destroys the data.

Michael Ellis: It is not like “Mission Impossible”.

Daniel Thornton: Almost.

Q208 Lord Faulks: Do you think that the ability to access communications data reduces the amount you would otherwise be spending on investigations? In other words, is access a significant cost benefit, or not?

Daniel Thornton: I find that a very difficult question to answer. It is a unique and central tool, so it is not a question of having an alternative technique to get the same information. The premise of the question does not really work for our sorts of investigations, because you simply would not be able to detect the connection rather than have an increased cost to try to find it.
Nick Tofiluk: From the commission’s perspective, the position is similar in the case of looking for organised crime related to match-fixing and insider information, but, in the case of what you might call bricks and mortar-type investigations, the consequence may very well be that our only real alternative would be to use some form of directed surveillance, which would possibly add tremendously to the cost. I have personal doubts whether it would be that effective, and it might be even more intrusive than our current mechanisms.

Q209 Lord Faulks: More costs in terms of manpower.
Nick Tofiluk: Absolutely.

Gillian McGregor: For the Border Agency it is quite difficult to quantify, but there are two angles to this in terms of cost. One is very similar to the point made by my colleague from the Gambling Commission. If we did not have access to this communications data, we might need to consider more resource-intensive direct surveillance activity, which would be very time-consuming and costly. We would also have to consider carefully whether we investigated certain serious crimes.

Lord Faulks: Because you did not have the resources.
Gillian McGregor: Yes. That brings its own cost in terms of both the cash seizures that might follow a successful prosecution but also the general cost to UK plc as a result of increased crime. We can attempt to do that if the Committee would find it helpful, but it is quite difficult to quantify.

Councillor Bettison: We do not carry data on that, so I am not able to assist.

Q210 Lord Strasburger: All the discussion so far has been about the use you make of data obtained under RIPA and your desire not to lose access to that, but you will be aware that this draft legislation substantially expands the range of data that would be available to public authorities. Is there any of that expanded data, and if so, which, that you feel would improve the ability to do your job?

Gillian McGregor: My view would be similar to that of my colleague from the FSA. We do not know what we do not know, but our sense is that the serious criminals we are dealing with on the immigration and customs side are making increasing use of more sophisticated internet and smart phone techniques to communicate. It would potentially give us more options, but the same considerations of proportionality and necessity would apply. The agency is looking to retain the ability to keep up with the communications used by the criminals we are dealing with, and we understand that because technology is progressing the current information is perhaps not the whole story.

Nick Tofiluk: I agree with the point about the sophistication of those we are trying to find in disguising their footprint, but from the commission’s perspective we are entering an era where the remote gambling platforms are of increasing sophistication, not least because of what we call peer-to-peer gaming. A global internet room means that communication is taking place not only through different technologies but over international boundaries. We are looking at the potential for things like money-laundering through techniques that enable peer-to-peer gambling, or playing through exchanges. In one sense we do not know what we do not know yet, because we are in a process of discovering exactly what techniques are being used to pass information, what technologies are being used and what the fundamental difference is. This is going to pose as much of a challenge for us to define what it is to CSPs, so they are on the lookout for it, as it is to describe it to ourselves to capture it. From the perspective of the Gambling Commission, a period of dialogue is coming, possibly through the engagement of ACPO’s Data Communications Group and the CSPs, about the exact nature of the information now being transacted in what can broadly be called fraud through gambling. We would start by needing to define “capture”.


Q211 Mr Brown: I want to return to the point about warrants. Councillor Bettison, are you able to tell us what proportion of warrant applications are rejected by magistrates?

Councillor Bettison: No, but I am sure that we would be able to come back.

Mr Brown: Would you be able to supply that to the Committee?

Councillor Bettison: Yes.

Q212 Lord Armstrong of Ilminster: I think your answer will be different from Councillor Bettison’s. You must have a designated senior officer to authorise an application. How many of these people do you have in your organisations? Are they employed solely on that, or do they combine it with other roles?

Daniel Thornton: Our processes are quite similar to those of other law enforcement agencies. We have a dedicated single point of contact and his deputy, both of whom are highly trained and work in a secure area. They are the first gatekeeper, if you like, for applications. The designated persons are heads of department in the Enforcement and Financial Crime Division, who are well used to managing complex financial services investigations and judging proportionality and necessity, which they have to do in their daily jobs in respect of how we exercise our statutory powers more generally. This is not the only intrusive power we have into data. That is how they fit in. The senior responsible officer is me. There are also lawyers involved in a lot of the steps in the process. We have lawyers in the investigation teams. The SPOC is looked after by a lawyer who assists in any legal issues arising. The majority of our heads of department are also lawyers and I am a lawyer. We are probably a bit lawyer-heavy, but there is a great deal of legal oversight in the whole process.

Lord Armstrong of Ilminster: Are your senior designated officers sufficiently detached from the individual cases?

Daniel Thornton: Yes. You cannot be a senior designated officer on a case you are managing or are involved in, so there is independence from the investigation that is being conducted.

Q213 Lord Armstrong of Ilminster: Councillor Bettison, this may be a difficult one for you.

Councillor Bettison: It is perhaps slightly different. Because of the level of data requests submitted by individual councils, it would not be feasible to have an officer dedicated solely to approving requests for communications data. Senior officers, although still an integral part of the service or legal support associated with the detection and prevention of crime, are required by RIPA to be designated officers, and their standing within the local authority is that of a director, head of service and service manager. All RIPA-style activity is also overseen by elected members. As responsible employers, all councils ensure that these individuals are very well trained, although it is not their sole purpose in the authority to do this, as I mentioned earlier. We take it very seriously, and, in the final analysis, the elected members are responsible.

Q214 Lord Armstrong of Ilminster: Presumably, the number of designated officers will vary according to the size of the authority.

Councillor Bettison: In most authorities it would be one.

Daniel Thornton: For us, it is seven.

Gillian McGregor: The Border Agency has an arrangement very similar to that of my colleague from the FSA. We have a single point of contact, which is a very small secure unit that brings in all the requests. They are referred to the designated senior officers, of whom we have 18 across the whole agency. It is a relatively small number for an agency that employs
thousands of people. They are all people who are regularly involved and highly trained in investigations under RIPA, but, as with my colleague, there is a very clear dividing line. An application that could be considered by the senior officer must not be an investigation in which they are involved. We find that quite easy to manage. Our agency is based nationally, so it is very easy to separate the investigation from the designated senior officer who would approve or otherwise the request.

Nick Tofiluk: The commission is very mindful that you might be involved in the war but the rule is that you are not involved in the individual battles. We have two fully trained single points of contact within the secure intelligence environment. They are trained by the National Policing Improvement Agency and accredited to the same standards as the police. We have four designated senior persons, one of whom is not the head of enforcement, to enforce that separation. All are trained, and three of those four have previous experience either with SOCA or the police and have gone through training there and have had responsibilities in those environments. The senior responsible officer is myself, and the unit is led by the head of intelligence, which has responsibility for wider information management as well as RIPA.

Q215 Stephen Mosley: You have been talking about internal monitoring. From the external point of view, can you talk about the process of the Interception of Communications Commissioner that you have seen?

Daniel Thornton: We have had several visits, probably every 15 to 18 months. One of his inspectors comes for two days, does a very thorough review and looks at many requests. We have always come out well from our inspections, in that all the applications looked at have been lawful, proportionate and necessary. We see it as a very thorough process.

Q216 Dr Huppert: I declare an interest as a vice-president of the Local Government Association. I am struck by what we have heard already. Despite the focus and rhetoric on how powers to access data will be reduced to four key organisations, it seems that you have all had discussions with the Home Office about expanding it again. I can see how these things balloon. On the face of the Bill, the Local Government Association is in the rather odd position of not being included but having constraints on the powers it could exert if it was to be included, whereas the rest of you are just not in the Bill at all. Do you support the fact that the warranting system was introduced? Are you concerned that it might put off local authority officers from requesting data?

Councillor Bettison: We are not concerned that they would be put off requesting data. They request data so infrequently that it is already of such importance, and if that is the price we need to pay we will pay it.

Dr Huppert: You support the warranting system.

Councillor Bettison: Yes.

Q217 Dr Huppert: That is very helpful and clear. The rest of you are in the odd position of not being included on the face of the Bill but also not having any constraints. Given the relatively small number of data requests you all make, it seems that, like the Local Government Association who accept the warranting system, that could be made to work for you as well. Would you be comfortable with such a system?

Daniel Thornton: I do not accept that. The volume of our requests is quite significant. To introduce a warranting system, even if it was for only the more intrusive forms of data—i.e. not just subscriber data—would be quite a significant change from our processes. You can judge whether or not it is necessary in terms of the robustness of our processes, but to have to go to a magistrate means it would probably be at least once every working day for the amount
of requests we are putting through. It would be quite a considerable burden. Our other significant concern about introducing that sort of system is the likely delay caused to investigations. We are not dealing, except in exceptional cases, with very urgent applications. It is not like going for a search warrant, for example, which can be done in a few days. These might get to the bottom of the pile. If they are going to take weeks, there is a danger of significantly prolonging the investigations and our being unable to get access to data at all, because it will drop off the end of the 12-month period, not to mention the cost and expense of this sort of process. It is not like we would be doing one a month; it would be much more frequent.

**Dr Huppert:** Any system would have to be prompt and efficient for it to work for you.

**Daniel Thornton:** Yes.

**Q218 Dr Huppert:** What about the other two agencies?

**Gillian McGregor:** I would completely echo what my colleague from the FSA said. We have similar issues. Our volume of requests, although a small percentage—it is about 1% of the total—is still quite a significant number. We would find it very challenging to operate the warrant system in terms of the capacity and cost that might be involved, but also there would be potential delay in cases. A number of our cases—not all—require a response to very urgent situations, including high-harm subjects and, in certain circumstances, a risk to life, for example trafficking cases, or dangerous people who have breached the border.

**Nick Tofiluk:** Our volumes are relatively low, and, therefore, I would not be in the same position as colleagues who have spoken already. There would be a cost implication for us in terms of a small organisation. The issue of delay would be a concern to me, although we are not in the territory of threats to life, but again we would, more than likely, go a court in the centre of Birmingham, which may very well be having a lot of other requests given the nature of the city and other organisations in that area, so there is the issue of delay. I would ask what value that would add, not least because, as colleagues said in the previous session, we would retain our internal scrutiny and oversight. I am not questioning the principle, if that is the wish.

**Q219 Dr Huppert:** Do you all accept there is a fundamental issue about self-authorisation for powers versus external authorisation? You are presumably aware that almost every other country with a similar process has some form of third-party authorisation. Do you accept that principle at least?

**Nick Tofiluk:** There is a question about transparency and whether we have faith in the oversight arrangements at the present time. That is not for me to answer in that sense. If it is the will of Parliament that there is transparency through the courts, quite rightly that would be accepted, but, as police colleagues also said, that would not mean our internal arrangements would be any the less robust.

**Q220 The Chairman:** When the new National Crime Agency is set up, will UKBA become part of it, or does part of UKBA link in with it in pursuing investigations?

**Gillian McGregor:** The agency will remain separate. We are part of the Organised Crime Partnership Board with the police, SOCA and HMRC, so we are very closely linked with the National Crime Agency. There will be a border policing command aspect to the National Crime Agency, but the UK Border Agency will remain a separate organisation.

**The Chairman:** That is helpful. You have clarified what I imagined was going to happen. Thank you very much. I am sorry we are running slightly late. We have had an excellent evidence session again, and we very grateful for the information you have given us.