Joint Committee on the Draft Investigatory Powers Bill

Oral evidence: Draft Investigatory Powers Bill, HC 651

Monday 30 November 2015

Watch the meeting

Members present: Lord Murphy of Torfaen (Chairman), Victoria Atkins MP, Suella Fernandes MP, David Hanson MP, Shabana Mahmood MP, Stuart C McDonald MP, Dr Andrew Murrison MP, Matt Warman MP, Baroness Browning, Lord Butler of Brockwell, Bishop of Chester, Lord Hart of Chilton, and Lord Strasburger.

Questions 1-38

Witnesses: Paul Lincoln, Director, National Security, OSCT, Home Office, **Richard Alcock**, Director, Communications Capability Development Programme, OSCT, Home Office, and **Lewis Neal**, Director, Intelligence Policy, Foreign and Commonwealth Office, gave evidence.

Q1 The Chairman: I apologise for the fact that we are two minutes late. Welcome to our witnesses. We have, of course, seen Mr Lincoln in another capacity. We have until between now and about 5.30 pm. As is normal with these arrangements, all members of the Committee will ask questions. I will kick off in a second, but I remind Members of the House of Lords that they should declare any interests when they ask the question. Perhaps I could ask the three of you a very general question to begin with. Could you give a few brief remarks on what the draft Bill proposes and why it is necessary?

Paul Lincoln: The draft Bill responds to the three reports that were commissioned in this area: the recommendations from the Independent Reviewer of Terrorism Legislation, David Anderson QC; the review that was done by the Royal United Services Institute at the behest of the then Deputy Prime Minister; and the report by the Intelligence and Security Committee of Parliament. All three reviews agreed that the powers associated with communications and the data associated with communications should be brought together in one place to make them more clear and transparent. This draft Bill attempts to do three things. First, it brings together, as requested, the powers already available to law enforcement in this area. It makes them clearer and more understandable than they have been in the past. Secondly, the draft Bill overhauls the oversight arrangements. In particular, you will have noticed that we have proposed a double-lock authorisation for the most intrusive powers, which consists of a Secretary of State authorisation as well as a judicial commissioner authorisation. Thirdly, the Bill ensures that the powers are fit for the

digital age, so restoring capabilities that law enforcement would previously have had in relation to communications data by bringing in powers for internet connection records.

The Chairman: Thank you very much. I do not know whether your colleagues wish to make any additional points. If not, arising from that and to make it clear to the Committee, which of the proposed powers are brand new, and which of them are being rewritten in new legislation?

Paul Lincoln: This Bill is very much about transparency and oversight, which the three reviews all said needed to be improved, as this is about powers. The Bill brings the existing powers together. The only new capability that is provided for relates to internet connection records.

The Chairman: Yes, but what does that mean for oversight?

Paul Lincoln: It not only brings the double-lock system that I talked about for the most intrusive powers, involving Secretary of State and judicial commissioner authorisation, but it establishes a new Investigatory Powers Commissioner, bringing together the existing three commissioner bodies and providing additional resources and additional technical and legal expertise.

The Chairman: Thank you very much. Other than the expiry at the end of 2016 of the provisions of DRIPA, what would the impact be if we did not have this Bill?

Paul Lincoln: If we did not have this Bill, we would lose a once-in-a-generation opportunity to provide some of the additional oversight mechanisms that I talked about a moment ago. In terms of the powers and capabilities, a new capability is provided for that in effect restores powers that used to exist around internet connection records. We have provided data as part of the associated documentation with the Bill, which sets out the operational case for that.

Q2 The Chairman: Just one more question from me before I hand over to my colleagues. What has been the impact of the Digital Rights Ireland case and the Court of Appeal decision in the Davis case on the powers and the wording of the Bill before the Committee?

Paul Lincoln: The Government responded to the Digital Rights Ireland case by passing some fast-track legislation in 2014, the Data Retention and Investigatory Powers Act, which took account of the ruling on Digital Rights Ireland. However, on the back of that, a judicial review was brought against those powers, which Parliament had voted for. That judicial review, in the Divisional Court, found two reasons for which the powers were incompatible with European legislation. Since then, a Court of Appeal ruling has said provisionally that it did not think that Digital Rights Ireland set out a minimum set of standards for Governments to comply with, and on the back of that the Court of Appeal has remitted this to the court in the European Union. Therefore, we have considered that position and the powers and the associated processes for which Parliament voted in 2014.

Q3 Lord Strasburger: Could you tell us in which Acts there would still be surveillance, data acquisition or equipment interference powers after the passage of this Bill?

Paul Lincoln: We have taken the opportunity to bring those into this, when it comes to the primary purposes relating to accessing communications data or content, but the Police Act, for example, would still allow equipment interference for other purposes.

Lord Strasburger: Are those the only ones?

Paul Lincoln: Those would be a good example. Similarly, the Intelligence Services Act would allow that for the intelligence agencies.

Lord Strasburger: Will you be able to give us a list in writing?

Paul Lincoln: We can write to the Committee.

Lord Strasburger: Secondly, you indicated that all the powers except one already exist. I think that we need a bit more clarity on that, particularly about whether all the existing powers have been recently authorised by Parliament. Given that CNE was not avowed by the Government until February 2015, bulk interception was first mentioned in the ISC report in March 2015, and the collection of bulk communications data was not avowed until the Home Secretary did so this month, it would have been impossible for any of those, as well as several other powers in the Bill, to have been specifically debated and authorised by Parliament. Do you agree that it is high time that many of those existing powers were debated by this Committee and by Parliament?

Paul Lincoln: The powers exist already. As David Anderson said, this Bill is an opportunity to bring that more clearly into focus and to allow Parliament, as we take this forward, to take an explicit view on all the powers in the Bill.

Lord Strasburger: I think you missed my point, which was that the three powers that I mentioned and others have never been specifically debated in Parliament. Do you not think that it is time that Parliament did debate them?

Paul Lincoln: Parliament now has the opportunity to debate these powers as this Bill is passed.

Q4 Suella Fernandes: What is it about the character and scale of the threat that makes this legislation necessary?

Paul Lincoln: If people look at the products in the public domain, the Joint Terrorism Analysis Centre has independently set the level of threat to this country at severe, which means that an attack is highly likely. You have also heard that the Home Secretary, the Prime Minister and the intelligence agencies have said that seven plots against this country have been disrupted this year that otherwise would have ended up probably in some form of fatality. Equally, figures published worldwide indicate 12,000 terrorist attacks in 91 countries in 2013, the last year for which figures were publicly available.

Q5 Shabana Mahmood: How confident are you that the powers in the draft Bill are effectively future-proofed?

Paul Lincoln: By bringing the powers together we have looked at the question of future-proofing. The critical thing is internet connection records and restoring capabilities that law enforcement have traditionally had as part of that. Richard no doubt will talk later

about some of the processes that we have been through in talking to communication service providers and other technology companies about the specifics of the technology.

The Chairman: Let us move now to Mr Hanson, who I know has a number of questions.

Q6 Mr David Hanson: As regards the old system versus the new system of judicial authorisation, I am interested in whether there is any likelihood of additional time pressures on decision-making.

Paul Lincoln: Each authorisation is currently considered on a case-by-case basis, and that takes a certain amount of time. There is no set time for looking at the authorisation. It needs to be done on the merits and the complexity of the case. Additional time may be needed for physically having two people involved in that decision-making process. The system that was put in as part of the draft Bill allows for urgency procedures. If there is a time-critical situation, a judicial commissioner can sign off under that procedure up to five days afterwards.

Mr David Hanson: Could we expect that, for example, in the Christmas period, the new year period or Easter period? Is that feasible and doable? In an urgent circumstance, would that be acceptable?

Paul Lincoln: In urgent circumstances, we have systems now in place where we deal with Secretaries of State. We have rota systems in place and we can access Secretaries of State out of hours to work through those systems.

Mr David Hanson: In the event that the judicial commissioner disagrees with a recommendation from a Secretary of State, what is the mechanism for that to be examined? Is that it?

Paul Lincoln: If that happened, the judicial commissioner would have to set out in writing the reasons for that refusal. The Secretary of State can have a discussion with that judicial commissioner to work through the issues. For example, it might be that collateral intrusion into a particular subject was too great when looking at necessity and proportionality. That is the kind of discussion that we have now.

If you got to a position where, having gone through that process, the judicial commissioner still disagreed, the Secretary of State can ask the investigatory powers commissioner to look at this. If the investigatory powers commissioner disagrees, that is as far as that will go and the warrant will not come into force if they disagree.

Mr David Hanson: What of that discourse would at any time eventually be public in the event of accountability for one or both of those officials being held by the House of Commons or the House of Lords?

Paul Lincoln: If something went wrong, as we have seen in the past, inquiries are often held. The Intelligence and Security Committee led an inquiry into the circumstances surrounding the murder of Fusilier Lee Rigby, for example, which took into account the way in which these things work. Similarly, the commissioners hold to account an oversight of the process that is put in place.

Mr David Hanson: One final question. How many of these do you estimate would be deemed to be urgent, given what happened historically? What is your assessment of the number that will be urgent?

Paul Lincoln: In reality, we think that this will be very few percentage points of the overall number of cases. We have not provided a specific estimate, but it will be a very small number of cases—probably the majority would be where there is an imminent threat to life.

The Chairman: What about the definition of urgency? Is it self-defining or will we have some sort of guideline? I am sure that there will be grey areas.

Paul Lincoln: We have not set out in the Bill a definition of urgent. In reality, a warrant will be considered urgent only if there is a very limited window of opportunity to act. We would expect to set out guidance in a code of practice, as is usually the way in which these things are set out.

Lord Butler of Brockwell: If a warrant has been issued—

The Chairman: I do beg your pardon. We have to adjourn for five or 10 minutes while Members of the House of Lords vote.

The Committee suspended for a Division in the House of Lords.

The Chairman: We were in the middle of a sentence.

Lord Butler of Brockwell: If a warrant is issued for one purpose, can the information that it provides be used for another purpose? For example, if a warrant is taken out for someone suspected of terrorism and it throws up evidence of offences under Customs and Excise, could the information be used without taking out another warrant?

Paul Lincoln: Certain purposes are set out for the intelligence agencies where they are allowed to share information along the lines of their statutory purposes. If I take your example the other way around, if you discover in a tax evasion case that someone was involved in terrorism, the practice would be that you would take out a separate warrant to do with the terrorism and run the necessity and proportionality test for that.

Lord Butler of Brockwell: Thank you. But the information that was first obtained under the tax evasion warrant could then be used to justify a further warrant for terrorism but a further warrant would be needed.

Paul Lincoln: A further warrant would be the practice to be followed through. Yes.

Q7 Dr Andrew Murrison: I am worried about the five days, because the Five Eyes community does not put up an artificial distinction between urgent and routine, since all warrants have to be certified by a member of the judiciary rather than a politician. I wonder why we have lighted upon five days. Are we seriously saying that we may not be able to get a judge to pass a view within five days? I would find that extraordinary. Perhaps we might consider whether a lesser period of time was appropriate for matters that are deemed to be urgent.

Paul Lincoln: Among the various recommendations from the reports, the Royal United Services Institute report, for example, recommended a period of 14 days for an urgency procedure, which we considered too long. We alighted on a period of five days as a maximum that would allow for sufficient time when the system may be running at its hottest if there was a particular set of counterterrorism investigations going on. In reality, we would expect decisions to be made much more swiftly than that.

Lord Strasburger: We know that the Home Secretary signs on average six of these warrants a day. Could you tell us approximately how much time she spends on it?

Paul Lincoln: I cannot give you the precise time that she spends on each warrant. She has said to the House of Commons that she spends more time on warrantry than she does on any other topic.

The Chairman: Thank you very much. We now move on to Baroness Browning, who has a number of questions that she would like to ask.

Q8 Baroness Browning: Thank you. I have to remind the Committee of my interest in the register as chair of the Advisory Committee on Business Appointments, which gives advice to senior members of the security and intelligence community when they leave office. Could I ask you about the request filter system, which I think is new? Could you explain to us how the request filter system works for applications to access communications data? In explaining how that works, perhaps you might like to give us an idea as to the correlation between the new system and fishing expeditions and whether there is a vulnerability there.

Richard Alcock: The request filter is fundamentally a safeguard, the purpose of which is to limit the amount of data that goes through to law enforcement. People access comms data right now through a system of robust oversight, with the appropriate checks and balances and with necessity and proportionality at its heart. The request filter cannot be used unless a particular case has been made that it is both necessary and proportionate. By way of example of how the request filter might be used, a criminal may have committed three crimes in three locations at three different times. A request for comms data may go in about who was at a particular location in those three instances. Without the request filter and subject, obviously, to the approval being granted for that kind of request, the full array of data would be made available to law enforcement. The request filter would filter out all the irrelevant data and just identify the individuals or entities that were in those three locations at that particular point in time, so it would reduce the amount of irrelevant information that would go through to law enforcement. It does not allow for fishing, just to address that point, because you can only make a request when that is necessary and proportionate for a specific instance, which is obviously judged by investigating officers and with the appropriate oversight.

Baroness Browning: You do not think there is any fishing risk at all in the system.

Richard Alcock: No, because the same tests apply to the existing comms data approval regime.

Paul Lincoln: It may be worth adding that the Bill provides for a new offence around the abuse of powers around communications data; it provides a criminal offence for people who abuse the powers as part of this.

Baroness Browning: The Joint Committee on the Draft Communications Data Bill, as you are probably aware, identified a risk to the request filter system. Why do you think there is a difference of opinion? What has changed to minimise that risk?

Richard Alcock: The Joint Committee concluded that it was a safeguard while acknowledging that there was a risk. The risk has been mitigated by virtue of the criminal sanction that may be imposed with inappropriate access to the information that could be accessed through the system.

Baroness Browning: Sorry, did you say "criminal sanction"?

Richard Alcock: The new offence, which Paul just outlined, of inappropriate access to comms data mitigates that risk.

Paul Lincoln: There is oversight by the Investigatory Powers Commissioner as a starting point in terms of all the powers in the Bill, but in addition to that we have greater defence in the Bill to make sure that in extremis if you are wilfully trying to abuse the system, a criminal sanction is available. There are also administrative and other sanctions available to the Government.

Q9 Lord Hart of Chilton: This is a question about judicial review principles. We know that the judge or judicial commissioner, when looking at the warrant, must apply the same principles as would be applied by a court on an application for judicial review. We have seen that there are some who say that that is not a great power because it is interested in process rather than the merits. I would like you to help the Committee by explaining what you understand to be the judicial review principles for the purposes of the Bill.

Paul Lincoln: As we said before, the Bill allows for a double-lock process. The judicial commissioner comes second in that process. The principle of judicial review is well established. Lord Pannick in particular set out that he thought that the test that was set for this Bill was the right one. In examining the data that is put in front of them as part of the request, they will see exactly the same information as the Secretary of State has and they will be able to determine whether or not the decision was lawful and rational. In doing so, they will also be able to determine whether or not the particular action was both necessary and proportionate. The necessary and proportionate test is, of course, exactly the same one that the Secretary of State is looking at.

Lord Hart of Chilton: We have seen David Pannick's article from 12 November, but we are interested in finding out the extent to which a judge could use what is called the Wednesbury principle in deciding whether or not no reasonable Secretary of State could come to the conclusion that a warrant was justified. Does the Wednesbury principle apply in this case, as that is a judicial review principle?

Paul Lincoln: The specifics here are that two things will be critical: first, that they decide in the first place that the action is rational and lawful; and, secondly, that it is necessary and proportionate. Those are exactly the same tests as the ones the Secretary of State will be looking at.

Lord Hart of Chilton: But how far could the judge go in deciding that the Secretary of State had stepped outside the remit?

Paul Lincoln: If a judge thinks that the Secretary of State has stepped outside the remit, it is for them to decide so and to say that they do not think that the warrant should come into force. Then there is the process that we described earlier about whether we appeal after that.

Lord Butler of Brockwell: What is the difference, if any, between "rational" and "reasonable"?

Paul Lincoln: I will have to ask one of my legal colleagues and write to the Committee on that one.

Lord Butler of Brockwell: It is an important point, because, as Lord Hart said, the question is whether the Wednesbury test—that no reasonable Minister could have taken the decision—should be applied. If I may say so, I do not think that you answered that. You used the word "rational", but what we really want to know is whether the Wednesbury principle applies.

Paul Lincoln: Okay. We will come back on the specifics of the principle.

Q10 Dr Andrew Murrison: On the subject of targeted interception warrants, if I had applied for and had been granted such a warrant but I wanted to change it in some way, how would I go about doing it?

Paul Lincoln: A process is set out as part of the draft Bill stating how modifications can be made to a targeted interception warrant.

Dr Andrew Murrison: Presumably those would be of a minor nature, or would they be fundamental?

Paul Lincoln: As for making a change to a warrant, if I was a criminal or a terrorist, let us say, and a decision had already been made by a Secretary of State and a judicial commissioner to put my communications under interception, then the decision had been made that it was both necessary and proportionate to intercept Paul Lincoln's communications in that manner. The example in that situation might be that I decide that I am going to buy a new mobile phone and, in doing so, I now have a new telephone number. Rather than necessarily going back and testing again that I am somebody who needs to have my communications intercepted, a senior official could make the change to say that that new telephone number could be added to that warrant.

Dr Andrew Murrison: At what point would you need to have the involvement of, first, the Secretary of State and, secondly, a judicial person?

Paul Lincoln: If you were to have situation where you then said—I do not know—a new person was coming along and a new circumstance, you would ask for a new interception warrant.

Dr Andrew Murrison: Through the whole process, so both the Minister and the judge?

Paul Lincoln: For both the Minister and the judge.

Dr Andrew Murrison: How does that differ from the situation that applies to equipment interference warrants?

Lewis Neal: It definitely needs some of the approach to modifications. Equipment interference follows the approach that we have taken to the original decision. In the case of SIA it will go through the departments of state, the Foreign Secretary and the judicial commissioner, whereas for law enforcement it will go straight to the judicial commissioner.

Dr Andrew Murrison: So why the difference?

Paul Lincoln: The approach follows the style point in how the authorising is done. In a case involving the intelligence agencies, for example, there is already someone separate from the chain of investigation who is looking at authorising that. In the case of the police, you are looking at doing this to add that additional safeguard as part of that process.

Dr Andrew Murrison: Presumably, there is also someone in the police looking at this too.

Paul Lincoln: Yes. Sorry.

Dr Andrew Murrison: You suggested that the difference was because in the intelligence agencies there is a specific person dealing with this.

Paul Lincoln: But you then have a separate department of state, which is independent from the body that is looking at it, which also considers that separately, whereas in the police you have that organisation itself looking at it rather than saying that there is a department of state, for example, separately looking at the authorisation. It is an additional safeguard.

Dr Andrew Murrison: Otherwise you just have the one.

Paul Lincoln: Otherwise you just have the one.

Dr Andrew Murrison: Do you think that is sufficient? It sounds a little odd to me.

Paul Lincoln: It effectively provides a form of a double-lock in terms of those modifications.

Dr Andrew Murrison: Why, then, should the handling of the equipment interference warrants and the targeted interception warrants be so different?

Paul Lincoln: That reflects effectively the starting point in saying who should be required to authorise that, and it follows consistently the starting point from—

Dr Andrew Murrison: It just seems to me that it unnecessarily complicates it.

Paul Lincoln: Our intention was to keep it simple.

Dr Andrew Murrison: Obviously it did not work. It has confused me. I admit that I am only a simple soul, but it seems to have established the two on different levels with different

procedures. I wonder whether the matter might be simplified by simply having the same process without distinguishing it.

Paul Lincoln: That may be a judgment the Committee comes to.

Dr Andrew Murrison: Would it be a major issue in terms of workload?

Paul Lincoln: We would obviously look at what the implications might be in detail.

Q11 Lord Strasburger: Why does the phrase "judicial review" in respect of warrants appear in the draft Bill?

Paul Lincoln: We have talked about that by saying that those are the principles under which a judicial commissioner would look at the authorisation of—

Lord Strasburger: I am just trying to understand why the judge would not look on the same basis as the Home Secretary.

Paul Lincoln: As I said, the consideration they will give follows the point about whether it is rational and lawful, and whether it is necessary and proportionate, which is the same test as the one the Home Secretary or the Foreign Secretary applies.

Lord Strasburger: So most judicial reviews are rather redundant, are they not?

Paul Lincoln: I think we said that we would write back on the specific principle. As I said, we are quoting both the report from RUSI, which said that this was an appropriate way to approach this, and some of the recommendations made by David Anderson. In this space, this seems to be the appropriate approach to take.

Q12 Suella Fernandes: Before the judge reviews a decision, how will the evidence before that judge compare to the evidence before the Minister?

Paul Lincoln: The judicial commissioner will have the same information as the Secretary of State.

Suella Fernandes: How does the test applied by the judge compare to that applied by the Minister?

Paul Lincoln: They will look at the rationality and lawfulness, and will consider the necessity as part of that decision.

Stuart C McDonald: Will the judicial commissioner be able to question members of the intelligence services, for example, when considering warrants?

Paul Lincoln: You would expect there to be potential for some conversation to go on. At the moment, conversations would happen with the agencies to try to clarify potentially the methods that people are using. If someone was trying to conduct surveillance or an intrusive activity against a particular suspect, you may question whether collateral intrusion was appropriate. Those are the kinds of conversations that happen now. You would expect similar conversations in the future.

The Chairman: To clarify that, when authorising a warrant, clearly the judicial commissioner and the Secretary of State need not be together physically. They could be in different buildings and different places, but would it be at more or less at the same time?

Paul Lincoln: When looking at the warrant itself?

The Chairman: Yes.

Paul Lincoln: Not necessarily. For more routine warrants, it may be a period of days before a judicial commissioner can do it.

The Chairman: Would that be the five days that we talked about?

Paul Lincoln: It could be a number of days.

Lord Hart of Chilton: Unlike the judicial review normally, there would be no third party representations, would there?

Paul Lincoln: The investigatory powers commissioners could look at the system and decide whether they think this is something on which they need further representation. We have not put a system in a place where we are expecting people to be making additional submissions on top of those provided. We have said that we will provide training to those who will become judicial commissioners, and we are working with the Lord Chief Justice's office to set out what that might be.

The Chairman: Who would look at the warrant first?

Paul Lincoln: The process is that the final person who has the say is the judicial commissioner. It will have gone through a Secretary of State first.

The Chairman: The Secretary of State and then the judicial commissioner.

Q13 Shabana Mahmood: I just want to look at the issue in relation to privilege. Obviously, Clause 16 relates to Members of Parliament and the additional safeguards that will apply to communications between a constituent and an MP. I was interested in the rationale for giving those additional safeguards for Members of Parliament but not for legally privileged communications between a client and a lawyer or the protection of journalistic sources. What is the reason for the differential treatment of all three things, which are quite important to our constitutional arrangements?

Paul Lincoln: The Bill provides now for all forms of interception. The requirement of a judicial commissioner to sign off is the key difference from the situation today. All forms of interception now require the involvement of a judicial commissioner. That is a significant step that people would appreciate. The difference with Members of Parliament is that it also requires consultation with the Prime Minister, which reflects the wishes of certainly Members of the House of Commons. There was a debate about that some weeks ago on the Wilson doctrine, which went to the Investigatory Powers Tribunal. This is the result of those debates.

Q14 Shabana Mahmood: Moving on to communications data, which is about context rather than content, as a lay person I would expect content to be the most valuable bit of what you might be looking for, but the context has also been described as gold dust. It is very important. How would you describe the relative value of context as opposed to content when it comes to communications data?

Paul Lincoln: Both forms are very important but in their own different ways. For example, communications data is used in 95%[1] of all criminal prosecutions. It is an essential tool for law enforcement in particular to identify, for example, missing persons or to rule people out of an investigation and try to minimise more intrusive techniques to gain content from that. It is very valuable in its own right.

Shabana Mahmood: So the oversight regime is less stringent than it would be for content. Given that you are both saying that they are both valuable, why is there different treatment when it comes to oversight?

Paul Lincoln: Oversight is by the Investigatory Powers Commissioner in all senses and all the powers in the Bill. There is perhaps a question about the authorisation, which you talked about, where Parliament has traditionally said that communications data is a less intrusive form than content, and the authorisation regime that maintains a very similar process that we have today reflects that.

Shabana Mahmood: Do you agree that it is a less intrusive form?

Paul Lincoln: Personally I do, and the Government have reflected that in the way in which the Bill has been put together.

Shabana Mahmood: Is that view shared across your sector, as it were?

Paul Lincoln: Yes. Law enforcement and the intelligence agencies will say that that is the same.

Q15 Shabana Mahmood: What is the rationale for Schedule 4? I can understand why police forces and intelligence agencies need to have access to communications data or are entitled to see acquisition of the data. I was slightly nonplussed by local authorities being on that list, given that by 2020 it would be a big deal if they can trim a tree or fill a pothole, rather than acquiring communications data, which might be beyond their resources.

Paul Lincoln: A wide range of bodies have access to communications data. The Financial Conduct Authority might use it for conducting investigations into insider trading. The Maritime and Coastguard Agency might use it for finding missing people at sea. For local authorities, ways in which to investigate might include rogue traders, environmental offences or benefit fraud.

David Anderson said that if you have relevant criminal investigation powers you should have the tools associated with that, and communications data is one of them.

Lord Hart of Chilton: Just one point. I did not quite get the answer to the question about the justification for allowing legally privileged communications to be intercepted. As you

[1] Witness correction: the figure refers to 95% of serious and organised crime cases, handled by the Crown Prosecution Service

probably know, the Bar Council has raised strong objections to the fact that privileged communications between an individual and a lawyer are not safeguarded. Why is that?

> **Paul Lincoln**: Special considerations apply to legally privileged material. Their safeguards are set out in codes of practice as part of this. Unfortunately, there may be situations in which people try to abuse the privileges available to them. Therefore, there is not a complete bar on such activity in terms of interception.[2]

Lord Hart of Chilton: Some might not consider that to be sufficiently justifying it, but that is the answer. Thank you.

Q16 Lord Butler of Brockwell: I understood that the Home Secretary said in her statement that local authorities would no longer have access to communications data, and I cannot find them in Schedule 4. Could local authorities in certain circumstances select this data?

> **Paul Lincoln**: There are two points there. Local authorities have to go to a magistrate before they are able to access communications data. That was introduced in, I think, 2012. There have been some instances where potentially the powers have been abused. Part of the rectification of that was to bring in a magistrate.
>
> The second question is probably to do with internet connection records, where the Home Secretary is on record as saying that local authorities will not be allowed access to internet connection records for any purpose.

Q17 Lord Strasburger: Are you aware that most experts consider communications data, especially that including internet connection records, to be at least as revealing as content these days? A former NSA general counsel said that it absolutely told you everything about someone's life and that if you have enough metadata you do not need content. A former director of the CIA said, "We kill people on the basis of metadata". Do not the most intrusive elements in communications data need a higher level of authorisation than the current entirely internal process?

> **Paul Lincoln**: We agree that parts of communications data are more intrusive than others. As part of that, the Bill sets out the different authorisation levels, which are internal authorisation levels, with those that are more intrusive having to be signed off by a higher person in terms of the rank structure in any given organisation recognising the sensitivities behind it.

Q18 Dr Andrew Murrison: Can I just press you a bit on communications data and the long list of authorities that have access to this. I think you are referring in 2012 to the case that Poole Borough Council lost at tribunal, where it was found to have overstepped the mark.

---

[2] Home Office clarification: The policy intent is to make clear that special considerations apply to legally privileged material. The additional safeguards that apply to this and other particularly confidential information are set out in codes of practice. This is because the privilege attached to the contents of communications between lawyer and client is important and must be protected. However, it is in the nature of the intercepting agencies' work that they will sometimes legitimately need to intercept communications between people and their lawyers in the interests of preventing or investigating serious crime or terrorist activity.

Do you feel it is sufficient for these authorities to apply simply to a magistrate to gain the access that they say they require, or do you think that list needs to be revised? I certainly know which I think.

Paul Lincoln: Our approach has been to continue the process which requires a magistrate to sign off, which is an additional level to what it would be in other organisations. On top of that they have to go through a mandated single point of contact for quality assurance before going to make the request. The National Anti-Fraud Network is part of that, which has been pretty successful, and David Anderson recommends the NAFN as one of the most successful bodies in this area.

Dr Andrew Murrison: Do you feel that their access to this data will mean that their skills in other means of detecting fraud might become degraded? Do you agree that fraud covers a whole load of things from the most serious crime to the frankly trivial?

Paul Lincoln: To put the numbers into perspective, only 0.5% of requests made for communications data overall are made by local authorities. It is a relatively low number in comparison with investigations in the round.

Dr Andrew Murrison: That is no justification though, is it?

Paul Lincoln: For access in their own right?

Dr Andrew Murrison: Not ensuring the job that we have to do to scrutinise this legislation at this stage would not be justification for us to overlook this particular thing; simply to say that it is so small that it does not really matter?

Paul Lincoln: I was not suggesting that. But in terms of the safeguards put behind this, certainly the Government have responded to that previously, and we have kept the same method, which involves the magistrate and the single point of contact through the National Anti-Fraud Network.

The Chairman: Can we move now to Miss Fernandes? Is your voice holding up?

Q19 Suella Fernandes: I think it is getting worse. Why has 12 months has been chosen as the timeframe for data retention?

Paul Lincoln: You could choose a range of different periods for which you might have retention. The data retention directive previously allowed for a timeframe between six months and 24 months. The UK decided to adopt a maximum of 12 months when it first introduced its legislation in this area. The 12 months was considered to be the right balance as to the level of intrusiveness in holding that amount of data. It was done on the basis of surveys by looking into the way in which law enforcement used the powers.

The critical reason for going up to 12 months is child sexual exploitation cases. Certainly when a survey was done on this in 2012, 49% of all requests made in child sexual exploitation cases were for data between 10 and 12 months old. That is a very significant period, which is reflected in the position that we have taken.

Suella Fernandes: What assessment has the Home Office made of 18 months?

Paul Lincoln: You could go further than that, but this is the position that we have taken historically. Other nations have gone further. The Australians are a good example. They recently passed legislation to go for 24 months' worth of data retention, but we thought that 12 months struck the right kind of balance between those two things.

Suella Fernandes: In terms of communications service providers and their holding of data for 12 months, has there been any assessment of the cost and workability of that?

Richard Alcock: As you would expect, we have had a number of meetings with the communications service providers on which we would likely serve notice under the new legislation. The retention period in the Bill obviously reflects the retention period proposed in this legislation. We have a very good relationship with the CSPs on which we serve notices now. We have worked with them throughout the summer, and before then, to think about the likely data volumes and to work out the estimated costs for the retention of internet connection records specifically. Those are contained within the impact assessment.

It is important to note that it is an estimate. Why is it an estimate? That is because CSPs systems change all the time. There are mergers, acquisitions and so on, but it is the best estimate right now based on the work that we have been doing with them over the past few months.

Paul Lincoln: It is also worth clarifying that the period for a maximum of 12 months for communications data is already current practice in terms of data being stored by those that are under a data retention notice. So that is not a new proposal.

The Chairman: You said earlier that one of the reasons for the 12 months was the investigation into child abuse, but you also implied by that that other investigations might not need the retention for 12 months. Could there be a sliding scale of holding this material according to the nature of the investigation?

Paul Lincoln: There is a question, therefore, between retention and access. To be in a position where you can access data in relation to child sexual exploitation, you have to retain all data associated with communications for up to 12 months to able to make those connections. The question of access is then perhaps complicated in terms of practicality. You may end up missing a significant proportion of investigations. If I was to say that a firearms investigation needed data that was six months old, I might make a connection to a child sexual exploitation case that also needed nine to 10-months-old data, or to a prostitution ring that needed something else, and I would not necessarily be able to make the links between those different investigations by having access for different times.

Mr David Hanson: Can I just be clear? You said that the costs in the impact assessment are to cover the costs of the 12-month period. Are the Government entirely covering costs to service providers and any expanded retentions?

Richard Alcock: The costs are to cover reasonable costs for the additional retention of the internet connection records, so there is provision in the—

Mr David Hanson: So how much is the impact assessment figure? From memory, around £240 million is related to that cost.

Richard Alcock: It is £174 million over a 10-year period in relation to internet connection records. Right now, under existing legislation, in the last financial year we spent around £19 million on data retention, so broadly speaking we are doubling the cost of data retention.

Mr David Hanson: So, again, does the assessment over the 10-year period include an assessment of the expansion of the market, of different types of material, of different types of activity, of the capacity overall of organisations, of new providers entering the market? How do you arrive at that figure?

Richard Alcock: We have worked with industry over summer to look at the likely data volumes and the costs associated with that volumetric growth over time, so even though I gave the example of £17 million a year, the reality is that the cost may go up over that time. But, as I say, we have been working very closely with the comms service providers on which we are likely to serve notice to underpin the facts and figures within the impact assessment.

Mr David Hanson: So when we have the service providers in front of us in the near future and we ask them the same question, will they tell us that they are content with the amount of resource that they give them, or not?

Richard Alcock: As I say, we continue to work with the comms service providers to look at the estimates of volumetric growth and how we would go about implementing those systems over time. We make balanced judgments on the service providers on which we serve notices, and we sometimes have to make hard choices about where we put data retention notices. But, again, as I say, it is all about working very closely with law enforcement, to identify where most value can be accrued from retention, and with comms service providers to understand—

Mr David Hanson: One final question from me. Is that therefore a budget that you have to spend, or is that an assessment of the costs?

Richard Alcock: It is currently an estimate of the likely cost for implementing internet connection records over a 10-year period.

Mr David Hanson: With certain providers.

Richard Alcock: Yes.

Lord Butler of Brockwell: Why does the taxpayer have to meet the cost at all of these records being retained? Why can it not simply be a condition of providers providing services that they retain these records at their expense?

Paul Lincoln: What we have tried to do, and as we have done in the past, is to make sure that companies are not materially disadvantaged by having to meet the requirements of government in this space.

Stuart C McDonald: Just a quick follow-up question first of all. I was interested in what you said about doing surveys of police work in relation to retained data. You commented on the 49% of all requests in child sexual exploitation cases being for data between 10 and 12 months old. In how many cases where the data was between 10 and 12 months old did that data prove to be essential to the outcome of the case?

Paul Lincoln: You are probably better asking the law-enforcement colleagues who are giving evidence after us, but communications data is often the only start point for child sexual exploitation investigations.

Stuart C McDonald: Thank you very much. Also in relation to data retention, obviously one of people's key concerns is security. When you are retaining data on such a huge scale, how can you be sure that that data is going to be securely retained?

Richard Alcock: Our retention systems are built to meet stringent security requirements, working in partnership with comms service providers to ensure that they meet very rigorous standards. Those systems are overseen by the Information Commissioner. We have annual accreditation. We have, typically, dedicated stores in which the comms data is held, which can be accessed only by law enforcement through encrypted data links and so on. As I say, it is a high priority for us to ensure that security and integrity. We have a very good track record of maintaining the security of existing data retention systems, and we are looking very much to build on that good practice, working in partnership with the comms service providers.

Stuart C McDonald: A related concern is about the definition of service provider. Someone suggested that the way that is defined just now means that pretty much any form of software provider could end up being saddled with these obligations to retain records over 12 months old. Do you have a response to that concern?

Richard Alcock: We will not be putting notices on every service provider as you suggest; we make balanced judgments about which organisations we would serve retention notices. Obviously I cannot go into detail about the organisations that we would intend to serve notices on, but we have been working with every organisation that would be likely to have a notice served on it.

Paul Lincoln: It is also worth saying that there is a route of appeal for those organisations if they think that this is a disproportionate thing to do. They can appeal to the Secretary of State, and there is a process involving a technical advisory board, which will consider the technical implications and cross-implications as part of that.

Q20 Stuart C McDonald: My final related question is about whether or not it is going to place UK-based communications service providers at a competitive disadvantage, in that some non-UK citizens will simply choose not to trade with UK-based providers.

Paul Lincoln: Part of that question is similar to Lord Butler's question. In that respect, that is one of the reasons why we give reasonable costs back to the companies as part of that. Was there something else behind your question?

Stuart C McDonald: Not just in a financial sense but in the sense of the different obligations that are going to be placed on UK-based providers and non-UK-based providers. Some might

simply say, "If there is going to be all this storage of my data, I'm just not going to use a UK-based provider".

Paul Lincoln: The powers in this are not new; they have been known about for some time. Data retention is a widespread power that is used in many different countries, so I would think that that set of differentiators is likely to be limited.

Q21 Lord Butler of Brockwell: Going on to one or two technical issues, we understand that because IP addresses are not unique, you cannot identify a sender solely through the IP address, but you can identify them through the internet communications records: in other words, through what they have been to. So is it correct that providers keep records of internet connections?

Richard Alcock: Some do not at the moment. The purpose of the legislation is to ensure that they can where served under notice. The whole operation of communications over the internet is very complex. If you will indulge me, if you have a smartphone, that phone will then communicate with your comms service provider and you will have an IP address and what is known as a port address between those two nodes. There will then be another IP address and another port address between your comms service provider and the destination, whatever web service it is. So you have constantly changing IP addresses and port numbers, and because of that sometimes having the destination IP address or the internet connection record address is the only way of identifying a person to a communication.

Lord Butler of Brockwell: So have you reached agreement with the providers on how this is going to work technically? Do you have a clear agreement with them about what you are going to serve notices on for retention?

Richard Alcock: We have ongoing discussions with a number of comms service providers, as I mentioned before. Those service-provider systems are constantly changing. We have a good relationship with the service providers on which we are likely to serve notice, and we have a good understanding of their current technical systems. During all the conversations that we have with them, at no point have they said that it is impossible to implement.

Lord Butler of Brockwell: So when we see them, will we hear from them that they think that the exercise of these powers is practicable?

Richard Alcock: I hope they will say it is possible. They will say it is hard. They will say that there is more work to be done, because their systems are constantly changing. But, as I say, we have been having a productive dialogue with them for a number of months, specifically about internet connection records.

Q22 Lord Strasburger: Before I ask my question, I should mention that the Home Office estimate for the cost of implementing the communications data programme, which in terms of storage was considerably smaller, was, from recollection, £1.8 billion over 10 years.

I want to talk about security. There are many breaches of cybersecurity every week. Examples from the last few months include: TalkTalk; giffgaff; a 13 year-old boy hacking into the email account of the current director of the CIA and accessing sensitive government

data; and the theft of 4 million personnel records of US government employees, probably by the Chinese. How can the public have any confidence that their personal data, stored by the Government at their ISPs, will not be stolen, and who will be responsible when it is?

Richard Alcock: The retention systems are built to stringent standards, and those standards are set by the Home Office. Systems do not go live unless they have been independently tested and accredited. We are very confident in the arrangements that we have to maintain security of the data retention systems, and I cannot say more than that. We completely understand the threat, and because of that we put a lot of effort into ensuring that integrity.

Lord Strasburger: Who advises on that?

Paul Lincoln: We do not want to sound complacent, but the Information Commission provides independent oversight of those arrangements. As I say, it is one of four principal things that we look at: the physical security of buildings, infrastructure and the rest of it; technical systems, including firewalls and the like; personnel vetting systems, where that might be appropriate; and procedure—the processes, training and the like, which are put behind that.

Richard Alcock: And all that is accredited on an annual basis.

Q23 Matt Warman: I would like to talk a bit about encryption. We all know that, on the one hand, encryption is absolutely essential for everyday life. On the other hand it has also meant that some bits of communication that you were able to access are now not visible. There is provision in the Bill for the Secretary of State to make regulations to impose obligations on telecommunications service providers "relating to the removal of electronic protection applied by a relevant operator to any communications or data". Does that mean that there is provision here to remove encryption, and, if so, how?

Paul Lincoln: I should start by saying that the Government are a strong supporter of encryption for information audit purposes and information assurance purposes. Some £860 million was spent on the national cybersecurity programme, and of course the spending review last week announced another £1.9 billion for looking at this. GCHQ probably does more for this country's cybersecurity than any organisation.

The Bill itself in effect replicates the existing legislation, which has been in place since 2000, and says in effect that we should be in a similar position to that of the real, physical world, where, as David Anderson says in his report and others have said, you do not want there to be places where people are allowed to go unpoliced and ungoverned. The same should apply in the internet world. So when you have taken the steps with regard to necessity and proportionality, you can place a requirement on companies to provide you with content in the clear.

Matt Warman: I understand that you might wish that to be the case, but in practice everything from my message from an iPhone to another iPhone is now encrypted end to end. Does this provision propose to tackle something like that, and, if so, how?

Paul Lincoln: Not everything is encrypted end to end. It would not suit the business models of many companies to encrypt their information end to end, and many of those

companies would not tell you that their systems were unsafe, which they are not. But you have to think whether or not in the right circumstances you will ask people to unencrypt information, and people do do that for us.

Matt Warman: Where companies currently think it is right to provide a commercial service that involves end-to-end encryption, are you trying to tackle that, and, if so, how?

Paul Lincoln: All we have done is replicate exactly the same service. If you are providing a service to UK customers and the Secretary of State and a judicial commissioner think there is necessity and proportionality in order to be able to provide that information, those companies should be required to provide that information in the clear.

Matt Warman: Do you think that is practicable?

Paul Lincoln: We are not setting out for anyone how they should do that. It is for others to say what the best way is for them to achieve that. The Government do not want to hold the keys to encryption or anything like that. That debate happened a long time ago. The Government decided that they did not want to do that and have not set out technical standards in this regard. They are saying, "In the right circumstances, we want you to be able to provide this information in the clear".

Q24 Matt Warman: I will come on to bulk equipment interference in that case. Could you all outline what bulk equipment interference is as far as you are concerned, and when it might be proportionate?

Lewis Neal: There is a difference between targeted equipment interference and bulk equipment interference. For targeted equipment interference, you might know the identity of the individual or the piece of equipment you are targeting. For bulk equipment interference, which is targeted at activity overseas and where the intelligence picture and the levels of information about your target are less, you would be able to seek authorisation to target equipment where you did not necessarily know a particular device or the individual that you were targeting.

Matt Warman: And when might that be a proportionate response?

Lewis Neal: Where you have a specific intelligence requirement overseas and you do not have the information but you might have an idea of the locality of the risk or the threat, the necessity would be set out and you would consider the proportionality of that action and potentially the types of information that you were seeking to obtain. Typically in that situation you might look at equipment data that enabled you to further identify the target and to develop a case for activities that have a higher level of intrusion.

Matt Warman: So you would see equipment interference in lay terms as happening at the level of internet infrastructure, rather than—

The Chairman: Order, order. There is a Division in the House of Lords. We will be back in 10 minutes.

The Committee suspended for a Division in the House of Lords.

The Chairman: Again, apologies for democracy. Perhaps I may move now to Miss Atkins who I know has a number of questions.

Q25 Victoria Atkins: How does the data collected as a result of equipment interference differ from interception material?

> **Lewis Neal:** Equipment interference is a range of techniques to acquire communication information from a variety of bits of equipment, from computers to mobile phones, whereas interception is making communications available while they are in transit. In practice you could use both tools to obtain the same levels of information, be it equipment data, communications data or content, but that would depend on your objective and exactly how you were using the tools.
>
> The legislation will require the agencies and the Secretary of State to consider the most proportionate way to acquire the data. If equipment interference may enable you to collect a certain bit of data, essentially you would use that technique as opposed to using interception where you may be collecting more data and a higher level of intrusion when it is not proportionate.

Victoria Atkins: Intercept material is not admissible, or indeed disclosable, in court legal proceedings. Why is it deemed acceptable for material acquired through equipment interference to be eligible for use in legal proceedings but not material acquired through interception?

> **Paul Lincoln**: In principle the Government have no objection to having interception used in evidence. It is the default that you would want to have material used in evidence, but there have been a number of reviews into this over the years. The last was in December 2014, which concluded that it was not possible to introduce an intercept-as-evidence regime in this country. The benefits would not outweigh the risks and the costs associated with doing so. There have been seven or eight reports on this, which have all come to that same conclusion.

Victoria Atkins: I know that colleagues might be wondering why intercept materials is admissible in other countries under different regimes. Is it fair to say that those countries have different disclosure regimes that perhaps are not as demanding of law enforcement and prosecution agencies as the disclosure regime in this country?

> **Paul Lincoln**: There is a combination of questions about disclosure. In particular, if you were to intercept someone's communications and were trying to use that in court, you would potentially need to intercept every bit of communication that they have done and transcribe all that so that you could set out whether or not there was information that was contrary to that that would be used to bring a prosecution. There are other ways in which other countries' regimes differ. We are not the only country in the world: for example, the Irish do not have an intercept-as-evidence regime either.

The Chairman: Thank you very much indeed. I am sorry that it has been a bit disjointed, but it has been an extremely valuable and interesting session. Many thanks for your time.

Lord Strasburger: Chair, may I correct my statement? I should have declared an interest. I have been a member of Liberty since I was a young man.

The Chairman: Thank you very much indeed.

Witnesses: **Simon York**, Director of the Fraud Investigation Service, HMRC, **Chris Farrimond**, Deputy Director Intelligence Collection, National Crime Agency, **Keith Bristow**, Director General, National Crime Agency, and **Richard Berry**, Assistant Chief Constable, National Police Chiefs' Council

Q26 The Chairman: My apologies for the late running of the earlier session. This was a consequence of Divisions in the House of Lords. You are very welcome. As you know, it is an extremely interesting and important Bill that the Committee is looking at and we very much look forward to the points you have to make to us. Perhaps I could kick off by asking your views on the draft Bill. From your point of view, why have it at all, and how will its proposals affect the work of your own organisations? In that context, which of the powers in the Bill would you regard as new, and which are to be simply consolidated into a new Bill?

Keith Bristow: Thank you Chair. Would you mind if I just made a few opening comments before getting to the specific question? First, thank you very much for seeing us so early. I am representing all senior leaders in law enforcement and policing, because we think this is so important that we need to come before the Committee quickly. Your team has also been very indulgent. I was anxious to bring three senior colleagues who are absolute experts in the breadth of law enforcement.

One of our deputy directors here is Chris Farrimond. He provides many of the law enforcement capabilities to which the draft Bill refers, including lawful interception, CNE and the high-end capabilities provided for the whole of law enforcement. He is a very useful person to have here.

Simon York from HMRC will be able to speak to serious criminality and the taxation system, which again demonstrates the breadth of some of the use that we have to put these capabilities to. Richard Berry is a very experienced police officer in a police force and leads for the National Police Chiefs' Council on communications data. He can speak in some detail about communications data and how it is used across a whole range of policing activities.

Why is this important? Technology has changed the way in which we all lead our lives, which is mostly a good thing for the law-abiding majority. But the reality is that serious and organised criminals in particular, who we target as an agency, also see very significant advantages from technology. That presents us with some very real challenges. The challenges come because the infrastructure of the internet provides some of these people with significant levels of anonymity, which is a challenge for us. The type of data that is stored and made available to law enforcement does not meet our purposes. The legislation within which we operate is not fit for purpose and was not designed at a time that reflected the age in which we live. The reality is that law enforcement is now experiencing a widening gap. We should remember that law enforcement work is evidential, which is different in many respects from other agencies—the SIA—and it is targeted. The

capabilities that we use are brought to protect the public but also to bring people to justice and to discount people and prove alibis.

In the Anderson report, David Anderson identified five purposes that we need for these operational capabilities. Those five purposes remain the same as when we spoke to David Anderson about them. The draft Bill goes a long way towards meeting our operational requirements. We recognise that our requirements are operational and need to be balanced against wider considerations that the Committee, the Government and Parliament in due course will take into account.

Nothing I will say is intended to cut across any of that. We simply want to set out what we need to keep the public safe. One particular concern to which I want to draw your attention—we can put some others in a written submission—relates to internet connection records. The challenge for us is that we believe we need access to all the data that is retained on internet connection records. However, in the draft form of the Bill, that will be limited to three purposes only, which means that data will be retained by communications service providers that we could not request.

As I said, this needs to be balanced against other requirements as well, but it is important to recognise that that limits some of our ability to protect the public and to fight crime.

Lord Butler of Brockwell: Sorry, you said three purposes. What are the three purposes?

Keith Bristow: This is not quite how it is worded in the Bill, but in operational terms one purpose is to resolve IP addresses. It is where a website contains illegal content—or what is called a communications website. For instance, codes of practice may help to refine this and develop our understanding, but it would not include a website where someone could book a rail ticket, which could be hugely important if it related to a missing person. We just need to be clear that data will be retained by service providers to which we cannot request access.

Chairman, you asked specifically about what new powers and new capabilities this Bill would give us. Frankly, it preserves the capabilities that we have always needed, but in a digital age it does not make us more capable of doing things. In operational terms, it brings up to speed what we need to be able to do in a digital age compared to an analogue age. A lot of what we will talk about is comparing what is acceptable to the public, expressed in legislation in the analogue world, how we need to be able to do that in a digital world and how the world has changed.

The Chairman: That is very useful. Thank you very much.

Dr Andrew Murrison: I do not understand this bit about the extra powers that you say you want to have. My understanding is that you could apply for those. Are you specifically talking about missing persons, because clearly you will be able to get a warrant to get information in relation to serious crime? I am left somewhat confused. Can you clarify it?

Keith Bristow: We cannot request data retained on internet connection records unless it is for the specific purposes that I mentioned. Let me give an example, and Richard is very well qualified to talk about this. If there is a vulnerable missing person—a young person perhaps—and we are concerned about what arrangements they may have put in place to go

abroad or to travel, we could not request access to an internet connection record to give us the lead to pursue that point.

Dr Andrew Murrison: Okay, but in relation to a serious crime, as presumably defined by the Serious Crime Act 2007, you would be able to request that data, would you not?

Richard Berry: If I can assist, sir, the major difference with this legislation is that the internet connection records would be retained. If data is retained, for example for business purposes, by a CSP—a communications service provider—then we can apply for that, but forward-facing. The big difference with this Bill is that there will be a retention of those internet connection records and, quite clearly, a process for us to apply for that.

Dr Andrew Murrison: So the information will be retained and you will be able to apply for access to it.

Richard Berry: Yes, but only for the limited categories that Mr Bristow mentioned: so, to resolve an internet protocol address—i.e. to attribute a communication; secondly, to establish whether a person has been using a communications site—Facebook, WhatsApp, those kinds of platforms; and, thirdly, if someone has been accessing illegal content—child abuse imagery or, indeed, terrorist material, that kind of material. There are other policing purposes that we would require access to internet connection records for.

Dr Andrew Murrison: What purposes are those?

Richard Berry: Well, for example; a banking website or, indeed, a travel website. There are case studies that we could furnish the Committee with in writing, if that would be useful, outlining some of those gaps. In a particular case in relation to human trafficking that involves booking flights and the movement of people, we would not be able to obtain that data under the provisions of this Bill. Perhaps I can speak from personal experience having run a large-scale anti-human trafficking operation where 85% of the actionable intelligence came from communications data. That was in the mobile phone era of 2008. We certainly could not repeat that kind of activity now, because the mobile internet communications platforms are where most people now communicate and do those transactions.

Keith Bristow: Might I add two things? Of course the codes of practice, when published, may help us to understand this, but this is our interpretation of the purposes that we can request internet connection records for, and those do not include some of what we will need to access, even though the data is retained.

Dr Andrew Murrison: I am afraid that I am rather confused, because for serious crime—the list is well laid out and, I think, well understood—my understanding is that you would be able to get that information. I am bewildered by what you say. However, there is a question, of course, about what further cases and crimes you may request information on. I think there would be some resistance to extending the list of serious crimes beyond that given in the 2007 Act, if that is what you are requesting.

Keith Bristow: I am not making any requests; I am setting out the consequence of our understanding, which would allow us to request access to data that has been retained by

service providers. You make a point about serious crime, but of course a missing vulnerable person is not a serious crime.

Dr Andrew Murrison: So to cut to the chase, is that your concern?

Keith Bristow: It is one of the concerns, but they are wider than that, because, as we understand it, we can only request data that has been retained by service providers for those three purposes.

The Chairman: So you are telling the Committee that to a certain extent the Bill does not do enough, as far as you are concerned.

Keith Bristow: The question that as law-enforcement professionals we are seeking to answer is: what do we need to protect the public? I am setting out what I believe we need to protect the public, but, as I said in my opening comments, Chair, we absolutely accept that there are wider considerations for this Committee, for Government and for Parliament to consider. I do not think, therefore, that it is for us to set out the operational choices.

The Chairman: You also indicated that any possible codes of conduct that might be constructed might resolve some of these issues.

Keith Bristow: I am not confident that they will resolve them, but they will probably clarify them.

The Chairman: Before Lord Butler asks his question, do any of your colleagues have any comments to make on this?

Richard Berry: Sir, if it would be helpful, the subsection that we are referring to is subsection (4) of Clause 47, which is entitled "Additional restrictions on grant of authorisations".

Lord Butler of Brockwell: I am puzzled, like Dr Murrison. Are we to understand that you could not request communications data to establish locations of suspected persons?

Keith Bristow: If it is for the three purposes that we have set out—

Lord Butler of Brockwell: Which are—

Keith Bristow: If it was a communications website, for instance, if we wanted the internet connection record for a Twitter or Facebook account—an account that is used for communication—we could request the data, and under the Bill the data would be retained and in a format that we could access. We are talking about websites that are not about illegal content, are not communications websites—bearing in mind that these terms are yet to be defined—and not IP resolution. Those are the areas where we understand that we could request access to the data that the service providers have retained on internet connection records.

Lord Butler of Brockwell: So we are only talking about internet connection records; we are not talking about mobile telephone records.

Keith Bristow: We are talking specifically about ICR.

Lord Butler of Brockwell: This is the distinction: we could still get mobile telephone records to establish the location of a suspect.

Keith Bristow: We could if a mobile phone was used as we currently understand it and as it has been used historically, but of course the really big challenge here is that people are communicating in a different way over the internet. We are confident in our interpretation that we could request access for communication sites, but our understanding is that we could not request the internet connection record of another type of website that might give us an investigative lead, such as one for booking travel tickets or banking.

Lord Butler of Brockwell: It seems to be a very big gap.

Q27 Victoria Atkins: Following on from that, would you still be able to contact let us say the travel agency, using your example, to ask whether it had business records to show that this request was made and that X number of tickets were bought?

Keith Bristow: More traditional investigative techniques could be used, but we need the lead in the first place on which travel agent we need to contact. Making the analogue-versus-digital point, the person will not have gone into somewhere on the high street; they will have interacted online. That will be the challenge.

The Chairman: It would be useful when this session is over if you gave us some written evidence with respect to some of the points that you have just made, because, as you can see, members of the Committee are interested in them.

Can I ask a question myself here? It regards current oversight powers. How do the investigatory powers that you currently possess work at the moment? What sort of oversight is there? Will there be a change as a result of this Bill?

Keith Bristow: I will ask Chris to deal with that question, but I will just make a remark to start with. We think that the authorisation and the scrutiny regime is hugely important, because public confidence is what underpins our ability to keep the public safe. It seems to us that because we cannot expose all our operational tradecraft, because we would be exposing it to the very people we want to tackle, we have to have a very clear regime that gives the public confidence that those sensitive techniques are being properly scrutinised. We think this is very important.

Chris Farrimond: There are two aspects to authorisation and oversight, and they are two quite separate parts. The authorisation process for some of our activities is internal, and some of it goes up to the Secretary of State. In each of those cases, whatever the investigatory power is, we go through a process whereby the applicant has to write down what they require, the proportionality, the necessity, the collateral intrusion, and give their justification. Then, whatever the application is—whether it is a police Act application for intrusive surveillance, a standard surveillance application, or an application for communications data—each application contains the same different aspects of the information: the proportionality, the necessity et cetera. It will then go through the various parts of the chain. It goes to an authorising officer in every case—as I say, in some cases it

goes right up to the Secretary of State. Those records are all retained and they are available for inspection at a later date.

We have two oversight regimes at present. One is provided by the Interception of Communications Commissioner's Office—IOCCO—and the other is provided by the Office of Surveillance Commissioners. The oversight regimes that they use are quite similar in that they come in for a pre-arranged inspection, on an annual basis for the most part, and we open up our records to them, give them access to our systems and let them see whatever they wish to see. For a period of a week, they will go through the records and pull out the ones that they want, and we will provide witnesses in the form of investigating officers, the applicants or whoever they wish to speak to. They will write a report based on that. Under the new legislation we envisage something that looks very similar, except that it contains one body rather than two, which we regard as fairly useful.

The Chairman: Thank you very much indeed. Moving to communications data, Miss Atkins.

Q28 Victoria Atkins: This is for all witnesses: how do you use communications data and for what purposes?

Richard Berry: If I might share the statistics with the Committee. Very helpfully, they were published on 20 November by the interception commissioner's office based on 100,000 communications data applications, so they are a really good data set. It varies massively. In this example, 80% of communications data applications are for the prevention and detection of crime, and 20% are submitted for interests of national security or, certainly in terms of vulnerable persons, to prevent death or injury in an emergency. So there is an 80:20 split there. From the 80% used for prevention and detection of crime, a quarter of those are in relation to police submissions for burglary, theft and robbery—volume crime.

Just under a quarter are for drug offences and just under 20% are for sexual offences. Then we have smaller and smaller chunks: 12% for harassment, 8% for homicide, fraud and deception, and violence against the person; and 1% for firearms offences. So there is a very broad spectrum of criminality.

Victoria Atkins: How valuable is this data to your investigations? I will come to prosecutions in a moment.

Richard Berry: It is essential, for example for establishing a lead, a seed upon which to build an inquiry. For example, if we take stalking and harassment, which is a very topical issue, around domestic abuse victims. To be able to establish a particular communication and an evidential line of inquiry around a victim being stalked, would be incredibly useful, in fact – vital, to support and corroborate an allegation.

Keith Bristow: We should remember that communications data for us in law enforcement is evidential. Sometimes we do not need to go any further than the communications data. We do not need to turn it into further authorisations for content. It is the "who, what, where, how".[3] Sometimes it is sufficient that we prove that to either eliminate someone

[3] Witness correction: clarification that what should have been said is "It is the who, when, where, how." What,

from our inquiries, to find a vulnerable person or to start the process of bringing an offender to justice.

Victoria Atkins: I will ask you about context and contact in the context of prosecutions in a moment. How valuable is it in relation to successful prosecutions?

Richard Berry: That can very much depend on the case itself. In a conspiracy case where communication between conspirators is part of proving the offence, it is absolutely vital. In terms of other offences, it could be considered vital. But it could also be important, for example, if we knew a particular person was in a particular place when an offence took place. We might use CCTV evidence to corroborate and identify that person in that location. It really depends on the particular offence being prosecuted and the nature of the evidence we are able to gather.

Q29 Victoria Atkins: Drawing together not just communications data evidence that deals with context but also cell site analysis of where mobile phones are at certain times of the day, is it possible to draw a timeline of a criminal offence in action that you can then present to the jury?

Richard Berry: Absolutely. It is commonplace now to produce a sequence of events—that is the term we use—and an analytical chart on the sequence of events showing communications and where people work geolocated by their phones, and to supplement that with other forms of evidence.

Q30 Victoria Atkins: Mr Lincoln mentioned very briefly an example of a warrant not being extended in circumstances where, for example, the target perhaps has got hold of another telephone. How common is that sort of activity in organised crime gangs?

Richard Berry: Operational security is as important to criminality as it is to law enforcement.

People regularly are changing their devices, setting up false accounts and swapping devices. All those tactics and techniques are used. It takes a lot of investigation to be able to understand who is using a device at a particular time, what it is being used for at that time and how it fits into the overall picture of that criminality.

Victoria Atkins: Just to get the point into context, the length of call can in itself help prosecution counsel when suggesting to a jury, for example, that that is the moment at which the drugs were dropped.

Richard Berry: Absolutely.

Chris Farrimond: I offer one or two other examples. One is about the range of use of comms data. The National Crime Agency receives the bulk of referrals in respect of child sexual exploitation on behalf of the United Kingdom. Just from one source, we receive about 1,500 per month. In many cases, resolving that IP address is the only way we can identify the victim or the perpetrator. I am sad to say that in 14% of cases we cannot resolve it at all. There is no way to do it and there is no way of identifying that victim or perpetrator. That is single-source intelligence and, if we did not act on that, there is no

---

refers to lawful intercept which is not incorporated in the meaning of communications data.

other way of doing it. We have similar examples, as will Richard, with missing children where there is no other way of identifying them but for this methodology.

Simon York: Can I give you an HMRC perspective on this? Last year, we made just over 10,000 communications data requests. That supported 560 investigations. I think that those numbers represent the complexity and the conspiracy involved in many of these cases. Almost 100% of our requests were in relation to preventing and detecting crime in contrast to the wider needs of the NCA.

This can be in relation to anything from smuggling to tax fraud to trying to criminally exploit HMRC's repayment systems. Literally billions of pounds are at stake here. Last year, investigations where we used communications data and intercept together prevented around £2 billion loss to the UK Exchequer. That is how important it is to us.

Victoria Atkins: Is it fair to say that a lot of those investigations involve serious organised crime gangs?

Simon York: Almost all of them, yes.

Q31 Lord Butler of Brockwell: Leading on from that, was I right to understand that you were saying that internet connection records although useful are not, as defined in the Bill, sufficient to help you to identify all senders, the users of all IP addresses?

Chris Farrimond: Some IP addresses are more difficult to resolve than others. A standard home broadband is a static IP and it is relatively easy to resolve down to an address. When you use your mobile phone, your IP address is allocated to that phone just for the few seconds that you make that search and then it is allocated to someone else somewhere else in the country. It is really complicated.

The IP addresses get swapped around mobile phones, tablets and everything else around the country a lot of times per day. Trying to get complete resolution for some of the more complex ones is not possible at the moment. We believe that ICRs will allow us to close that gap quite considerably.

Lord Butler of Brockwell: Right, but it will not close it completely. I understand that you cannot always resolve IP addresses, but if you get internet connection records you can identify the users of the address.

Chris Farrimond: I am afraid that my knowledge of technology is not good enough to give 100% on this, but we believe that it will massively close the gap. It could be up to the whole amount.

Lord Butler of Brockwell: Just going back to the three purposes for which you can use it, you say that you can attribute connection from an IPR. Then you could discover that someone had been a user of Facebook. How does it help in a criminal investigation to discover that they are a user of Facebook?

Chris Farrimond: It means that we can ask Facebook. Certainly, when we are talking about vulnerable children, threats to life or anything like that, we find that communication sites of that type are extremely helpful.

Lord Butler of Brockwell: If you go to Facebook, are you going to the content and not just the communications data? Would you seek a warrant? If you did seek a warrant, would that be effective with Facebook?

Chris Farrimond: At that stage we would not need to go for an interception warrant, because we would not be intercepting communications in the course of their transmission.

Lord Butler of Brockwell: I understand.

Chris Farrimond: It would be stored data at that stage, so we would be looking for the stored data that Facebook had in that instance.

Lord Butler of Brockwell: And Facebook would be able to tell you with whom the person who was suspected had been communicating with.

Chris Farrimond: It should be able to do that, yes.

Lord Butler of Brockwell: I understand. Thank you.

Q32 Stuart C McDonald: What would you say is the operational case for 12 months in particular being the maximum time for requiring the detention of communications data and internet connection records?

Chris Farrimond: I know that the Home Office, who were here before, gave you some figures. We have a table here that it might be helpful for us to include in our written submission to you, but let me give you some examples. In a 2012 survey right across policing in the UK, of all crime types within 0 to six months approximately 84% of comms data was applicable: that is to say, when we needed it, 84% fell within the 0 to six months, 13% within the seven to 12 months, and 3% in the 12 months-plus. But that does not give the whole picture. For child abuse, only 42% fell within the 0 to six months, and 52% fell within the seven to 12 months. There are also figures for terrorism offences, sexual offences and financial offences. We can give those figures, but this quite clearly shows that the closer you are to the date, generally speaking as soon as the investigators get hold of the case they are going to want to get the data, but sometimes it takes a bit longer, for whatever reason. For instance, we do not immediately get the referrals that I spoke about a few minutes ago involving child sexual exploitation; sometimes it can take a few months for them to come through, which may be the reason for the 52%. Either way, I think it shows pretty consistently that 12 months is a reasonable point at which to draw the line.

Keith Bristow: It is worth differentiating between types of investigation. As an agency and collectively, we sometimes investigate criminals; we are proactive, so we want to know how they were transacting at that moment. With reactive investigations, of course, often we do not know what data we need until an offence has been reported to us and we are some way down the track with an investigation. I suspect that is exactly why, with child abuse, data retention is further down the line in time terms.

Simon York: The position for HMRC is a little different. Our figures show that more than 50% falls into the six to 12 month period. Indeed, quite a lot falls beyond 12 months. We are doing a lot of reactive, or historical, analysis. We have some real-time stuff, perhaps

smuggling, but if it is more in the tax evasion area it can be a lot more historical; if it involves the use tax returns, we will not even do that analysis until 12 months after the year ends. We are in quite a different position from that of the National Crime Agency. Overall, we feel that 12 months is a reasonable balance to be struck, but we have a lot of cases that fall within that six to 12 month period.

Stuart C McDonald: Okay. We will obviously need to look in detail at the tables that you provide, but is there not a danger that what you are describing there is practice rather than what is essential. Is there analysis that shows that the information that you get from records that are between six and months old ends up being crucial to a case?

Richard Berry: If I may help with that, there are types of crime that require communications data perhaps two or three years after the offence has been committed and subsequently reported. Boiler-room fraud is a classic example of the picture of the criminality only emerges some years later, so clearly the 12-month period for the retention of communications data is not particularly useful for that particular criminality. Also, criminal justice processes kick in. If we are looking at an alibi or identifying further witnesses, subsequent applications for communications data up to that 12-month period can also be incredibly useful for a particular investigation because of the interests of justice and if the disclosure regime highlights that further inquiries are required by the police at that time. We have not mapped it, but I understand that that kind of data may be produced in the future and we can start to understand the value of data at a particular point in time for a particular crime type.

Q33 Stuart C McDonald: Thank you very much. Finally, as far as you are aware, how do such rights of access up to 12 months compare to rights of access that colleagues in other jurisdictions have?

Richard Berry: Our comparison is with the Australians, who have recently been given a two-year retention period. I understand that in the original period the data retention directive was for 24 months, so we are striking a balance in many respects. Twelve months seems to be the period when the optimal value is obtained by law enforcement.

Stuart C McDonald: In terms of internet connection records, this is fairly unique, is it not?

Richard Berry: We do not have that evidence.

Q34 Bishop of Chester: This is the first time I have spoken on this matter and I need to declare that I have no interests. Can I go to the question of the length of the period? Is there frustration that it is only 12 months in serious cases in HMRC, for example, where you cannot go back beyond 12 months? Australia has fixed two years. Is this a source of frustration to you in your investigation of crime?

Keith Bristow: I think there is a need to understand the mindset of the investigator. All the best investigators are rigorously focused on doing what they need to do to keep the public safe. Chris has given numbers demonstrating 0 to six months and six to 12 months. There are also numbers that show data after 12 months that would have benefited the investigation. My sense is that there is some science that points to 12 months, but there is also the professional judgment that, when you look at the numbers, the data appears to be less relevant after 12 months. Of course our mindset that is we want every opportunity to

protect the public in every set of circumstances, but that has to be balanced against other considerations.

Bishop of Chester: Are you sometimes slowed up by having to analyse seized equipment—laptops or whatever—which, as I understand it, is often in a queue, takes time and extends investigations?

Keith Bristow: Operation Notarise was an operation, led by the NCA and involving every police force in the UK, against people who were exploiting children online. We ended up seizing tens of thousands of devices that were relevant, which could be a digital camera, an iPhone: all the devices that we all understand. When you have that volume of devices, triaging those involves a lot of professional judgment about which are the most important to collect the most evidence from of the high end of high risk. We do not always get that right, because, frankly, there is not the capability, even with the private sector, to everything at pace all the time.

Bishop of Chester: Does the 12-month retention period hang over that investigation?

Keith Bristow: No, because once we have seized a media device, we have seized it. We then get to the point where we analyse its content. The 12 months is more about the data that is retained by service providers to enable us to access the data. It is not about the hard content of the device.

Bishop of Chester: So the analysis of the various devices that you have just described does not throw up the need to—

Chris Farrimond: It can do, because stored messages on a computer can point to an IP address, and, yes, we have had examples, even recently when they were one day over the date.

Keith Bristow: With victim ID, for instance, if we get an image and we want to identify the victim—a child who has been exploited—and we want to rescue that child, the reality is that we might need the communications data that sits around some of those communications to try to resolve the identity of the victim.

Q35 Lord Strasburger: The Counter-Terrorism and Security Bill earlier this year created the power to resolve IP addresses. How many times have you used that, and how does it differ from the power in this Bill?

Chris Farrimond: The provisions in that Act are not all in force yet. Although we use exactly the same communications service providers as our counterterrorist colleagues—so we use exactly the same access—we still cannot resolve the technology and the systems in place where the communications service provider has not yet caught up completely with the provisions of that Act. Therefore we cannot fully resolve all IP addresses, which brings me to the 14%.

Q36 Lord Hart of Chilton: Fifty-five years ago at university, I joined Amnesty International and I think that technically I might still be a member. That is my declaration of interest. What safeguards do you have in place to prevent unauthorised access to the

communications data and other materials you hold? I imagine that the criminal mind is always at work trying to break in.

Chris Farrimond: The vast majority of communications data is held by the communications service providers. We can only access it in the certain circumstances that I have outlined around necessity, proportionality etcetera, in which case in the NCA's case, it comes into the NCA and is held on the same systems as all the other evidence we have.

It is treated in exactly the same way, to the same specification and safeguards, as all our criminal intelligence data, which is held to a high level. Although there have been various attempts to get on our website, they have only ever managed to get on the outward-facing one. They have never managed to get anywhere near the inward-facing one. That is not a challenge. We are satisfied with the security of our system.

Lord Hart of Chilton: Just to be clear, how many break-ins have there been?

Chris Farrimond: I believe there have been one or two to our outward-facing website.

Lord Hart of Chilton: And how did they come about?

Chris Farrimond: I am afraid that, again, my technical knowledge defeats me.

Keith Bristow: As regards most of the attacks that we get on our outward-facing website, the catalyst is that we have taken on some cybercriminals. The community that supports people like that do a DDoS attack on our website to try to get us to take it down. We spend considerable resource and energy making sure we keep that site secure. That is not the system where we retain our intelligence and our evidence. It is the front face and it appeals to the public that we tell them what we are doing and are as transparent as we can be. We rarely take it down, but sometimes as the result of a DDoS attack we have had to do so to protect it.

Lord Hart of Chilton: How much has that cost you?

Keith Bristow: I would need to come back to you with a number, but it is significant.

Simon York: Similarly from an HMRC perspective, we hold this information on secure systems in secure buildings and we have specially selected and trained staff who are the only people with access to this type of material.

Lord Hart of Chilton: And you have not had any breaches?

Simon York: No.

Richard Berry: The single point of contact in David Anderson's report. they have pin numbers and they are all vetted to a high standard and they work in secure environments. There are a range of security measures, as well as the physical security, to ensure that there are no breaches of unlawful access of that information.

Lord Hart of Chilton: So, as far as you are concerned, there have been no breaches?

Richard Berry: Absolutely.

Lord Butler of Brockwell: The Inland Revenue had a notorious example of where they lost CDs in the post. Are you absolutely sure you have systems that prevent anything like that happening with this sort of data?

Simon York: Absolutely. After that event, which was quite some years ago now, there was a very comprehensive review of all our security processes. Interestingly, the data that was allegedly on those discs has never surfaced in any way to be used in criminality or otherwise in the UK.

Lord Hart of Chilton: Did you ever recover it?

Simon York: No.

Keith Bristow: From an NCA perspective, we invest huge amounts of energy and time in data security. What I could not do is give you a 100% cast-iron guarantee that there will never be a breach. When you mix well-intentioned people into any of these systems, it needs only one failing for data to get into the public domain. But within what is physically and legally possible, we treat this information security as our top risk.

Q37 Matt Warman: Can you talk me through what value equipment interference provides your organisation and what justification there is for you to be able to conduct equipment interference?

Chris Farrimond: We use property interference at the moment, which is authorised under the Police Act. We use it for a range of purposes, ranging from pretty much every-day relatively routine activities right up to far more high end. The difficulty is that trying to describe any of those techniques in this setting probably would be inappropriate, but I would certainly be very happy to explain them in a great deal more detail if we had the opportunity to do so.

Matt Warman: More generally, in that case, how often do anticipate being required to use equipment interference in the future?

Chris Farrimond: That is quite difficult to answer, because I could not have predicted the IP revolution that there has been or the digital change that we have seen. The change from traditional telephony into IP-based communications has been enormous and the pace has been really difficult to keep up with. I could not make any prediction about just how much we would use this. I suspect that our limitation would be around our own resources and our own capability rather than the demand. The demand for quite a lot of the services that I am allowed to manage within the NCA outstrips supply.

Keith Bristow: To give you a trend, I think it is fair to say that as law-abiding citizens it is no different—more of what we do now is online using digital devices. I imagine that the trend will peak, but I think that we will be doing more rather than less that reflects the behaviour of the criminals who we are targeting.

Richard Berry: To give a police perspective on this, we use equipment interference regularly, really for tracing vulnerable and suicidal missing persons.

The other point I would like to make is that there has to be some consideration from our perspective of the integrity of the information contained on a device that is interfered with. For example, to comply with the requirements of Section 69 of the Police and Criminal Evidence Act on the integrity of computer information, there might be considerations perhaps prohibiting the creation of data purporting to be communications data on that particular device or perhaps removing such data from that device. The evidential integrity of that device might be particularly important. Perhaps we can expand on that in a written submission.

Q38 Matt Warman: Finally, on demand versus supply, do your organisations currently have the capabilities technically and in terms of manpower to do what is needed? Do you anticipate seriously being able to ramp that up?

Chris Farrimond: We have the capability, and I anticipate that, if required, we could ramp it up, yes.

Keith Bristow: The change for the NCA and the transformation programme that it is going to go through—the Government announced the funding for that last year—mostly relates to our digital capabilities. As criminals go online, we need to be as adept in the digital environment as we are in the physical environment. Those capabilities are going to be invested in on behalf of the whole law enforcement community and not just us, because we provide those to our colleagues in HMRC, for instance.

Richard Berry: RUSI recommendation 5 as being that law enforcement should have a comprehensive digital investigations intelligence programme. A number of colleagues are here and we are part of that programme. Building capabilities is certainly one of those priorities.

The Chairman: Thank you very much indeed. Again, apologies for the delay because of the votes. This has been a fascinating session and we look forward to receiving your written evidence to supplement what you have told us today.

Keith Bristow: Chairman, do you mind if I just reiterate Chris's offer? We want to be open and transparent with the Committee and the public viewing this or reading the report are hugely important. However, we cannot betray all our tradecraft to criminals.

The Chairman: Of course not.

Keith Bristow: There is an open offer to the Committee, and I know that I speak for my colleagues as well; if you want to look at what we do, whether in a comms data unit or about equipment interference, we will brief you at a higher level of classification to help with your deliberations. Thank you for your time.

The Chairman: That is very generous of you. Thank you very much indeed.