



Home Affairs Committee

Oral evidence: [Regulation of Investigatory Powers Act 2000](#),
HC 711

Tuesday 4 November 2014

Ordered by the House of Commons to be published on 4 November 2014.

Written evidence from witness:

- [Interception of Communications Commissioner](#)

[Watch the meeting](#)

Members present: Keith Vaz (Chair); Nicola Blackwood, Mr James Clappison, Michael Ellis, Paul Flynn, Dr Julian Huppert, Tim Loughton, Mr David Winnick.

Questions 1 – 165

Witness: Rt Hon Sir Paul Kennedy, Interception of Communications Commissioner, gave evidence.

Q1 Chair: Could I call the Committee to order and welcome most warmly the Interception of Communications Commissioner? Thank you very much for coming today, Sir Paul. We are interested, in this very short report that we are doing on process, in how the office works and, of course, we have some figures already from your predecessor's report. I think we should place on record our appreciation to you for stepping in at very short notice following the accident of your successor.

Sir Paul Kennedy: We are very hopeful that he will return and progress so far has been very good. I spoke to him last week and he is capable of conducting a telephone conversation but I have not yet seen him.

Q2 Chair: Marvellous. The reason why we are concerned about it—and the public also appeared to be concerned—is the use of RIPA, which of course is central to what we are looking at today. We have seen figures that alarm us as to the increase in the number of warrants and the number of communications data items that have been processed.

Sir Paul Kennedy: Communications data have been roughly even at about the 500,000 mark over the last three years, if you remember.

Q3 Chair: Indeed, and thank you for reminding us. In particular, I have just received a reply to a parliamentary question relating specifically to the Home Office, which shows that the number of

communications data items processed by the Home Office has risen from 53 in 2002 to 6,056 in 2013. From your previous role, because we know you stepped in to do this recently, from the time you have been the Interception of Communications Commissioner, what do you think could be ascribed to this huge increase?

Sir Paul Kennedy: I think there are a number of reasons. One is that we live in a more dangerous world and the other is that as tools become available people become more used to their use and their limits. I think that in both those ways over a period of time you see a slightly greater use. What is important is that the use should be appropriate whenever it occurs and whatever the numbers are.

Q4 Chair: What is your role in ensuring that it is an appropriate use? How do you reassure Parliament that what they are doing is the right thing?

Sir Paul Kennedy: Can I move one step back? There is an important distinction—I am sure by now you are well aware of it—between intercept and data, and it is very important to keep that in mind because, of course, warrantry relates to intercept, to actually listening in to what people say or write. In relation to that, the role of the Interception Commissioner is, dare one say it, almost to mark the Secretary of State. The reality is the case for a warrant has to be put to a Secretary of State. By the time it gets to him or her it has been through a number of other people and hopefully the final presentation makes a good case for the issue of the warrant.

Parliament decided, when the legislation came into existence, that somebody should audit, come in afterwards, look at what had been done and decide whether or not it was appropriate, and that essentially is the role of the Commissioner. So he or she does not give permission in advance, has no hand in that, but we look at it afterwards, not on a 100% basis but on a sampling basis to see whether it was appropriately given. The same is true in relation to data, but there is no way in which I could look at 500,000 requests for data. It would be absurd.

Q5 Chair: That is very helpful. In respect of intercept, which you have just mentioned, how many have you looked at since the beginning of January this year?

Sir Paul Kennedy: The answer is that I only took over this role at the end of July. I have done one full-blown inspection since the end of July and, off the top of my head, something like 25 in relation to that particular authority. Can I just check?

Q6 Chair: Indeed. In the authority that you were inspecting, for example, you would have looked at 25 cases out of how many?

Sir Paul Kennedy: Forgive me, the number may be wrong but that is of the order, yes.

Chair: But what is that as a percentage of?

Sir Paul Kennedy: Overall, at the end of a calendar year it looks as though we do 10% approximately of the warrantry. I think I am right in saying that. It varies a great deal. It is quite difficult to put this picture over but in some agencies inquiries are long-running. I am now going back to my own experience before—

Q7 Chair: If we could hold the thought, the figure you have just given this Committee, that you are able to look at only 10%.

Sir Paul Kennedy: No. The reason I said 10% is you asked me how many I looked at. Can I just continue with what I was saying? I have to be very careful not to say things that may be of any assistance to people who perhaps should not hear. In some agencies inquiries are long-running and if, therefore, you are in post for a certain amount of time you will have seen most of the inquiries that that agency carries out. Can I take an example?

Q8 Chair: Can you hang on a second, Sir Paul? Sorry. We will come back to your examples. I asked you a specific question as to the numbers that you are able to see as a percentage. You said 10%.

Sir Paul Kennedy: I said 10% because that is in last year's annual report, as you may remember.

Q9 Chair: Yes, that is fine. So it is 10%. Don't you think that figure is very low? That means 90% are not even looked at.

Sir Paul Kennedy: No, I doubt it. I don't know what most accountants would say in relation to normal audits but I think it is high.

Q10 Chair: With respect, sorry, you are here to answer our questions and we will let you give us the answers. You don't think 10% is too low because you regard yourself on par with an auditor in an accountancy firm?

Sir Paul Kennedy: No, because you can make inquiries as to what you look at. As I said, I am only just back in it, but I would expect any agency to bring to the attention of the Commissioner any particular warrant that they regarded as of importance. In addition to that, of course the whole inspection would lose its tenor if the Commissioner did not dip sample, because you certainly do not want to be guided by the agency.

Q11 Chair: Indeed. So you would not expect them to say, "This is a difficult case. We would like you to look at it"?

Sir Paul Kennedy: Yes, they do that too.

Chair: They do? But human nature being what it is, they probably would not want to let you look at anything that they had hashed up, for example, would they?

Sir Paul Kennedy: I think we know when they have hashed up. They have to report errors and all errors are investigated in one way or another. One of the things that we have to do when we visit is to look at the error warrants, in other words the ones that—

Q12 Chair: Excellent. Finally from me, you are paid a salary of, I think, £150,000 a year. Is that right?

Sir Paul Kennedy: I am only paid by the day at the moment, may I say, so I am not on any salary at all.

Q13 Chair: What are you paid per day?

Sir Paul Kennedy: I am paid at approximately the half rate of a Court of Appeal judge.

Chair: Only Mr Ellis probably has any knowledge as to how much that is.

Sir Paul Kennedy: It is available in the—

Q14 Chair: Tell us about your staffing. We were concerned about the number of people you have to do this very important work.

Sir Paul Kennedy: The warrantry is a very important side but it is not, in terms of time, the big side. The big side, as the numbers suggest, is the data side.

Chair: Indeed. So how many staff do you have?

Sir Paul Kennedy: The answer is there are 12 in the office. There are nine inspectors, a chief inspector and head of office, and two support staff. The nine inspectors are out full-time visiting the areas where the powers are being used, for example a police force. When they do a big police force it will take three or four days; when they do a small police force or a small authority it will take one day. Are there enough? One is always a bit cautious but at the moment I believe there are. It is significantly more than the numbers who were there when I was in office up to the end of 2012 and that is because additional burdens have been put on the office.

Q15 Chair: How many years were in the post before you went off?

Sir Paul Kennedy: Six.

Chair: In those six years, in how many cases did you say you thought that the warrantry should not have been issued?

Sir Paul Kennedy: I don't remember ever saying it in those terms, but on the other hand that is not the way these things work.

Chair: How would you put it?

Sir Paul Kennedy: As I said to you at the very beginning, by the time a warrant gets to the Secretary of State it will have been through so many processes that it is very unlikely to be a warrant that he or she should not—

Q16 Chair: Using your own words rather than mine, in those six years how many times would you have said that you would not have regarded it as appropriate to have issued the warrant?

Sir Paul Kennedy: I don't think I ever said that. I think we discussed occasions when it was near the line and whether it should be renewed and whether it should be looked at after a fortnight or three weeks or something like that, which is the way these things operate.

Chair: Of course. So, none. Thank you very much.

Q17 Mr Winnick: Sir Paul, just to clarify your own position, you are interim, aren't you, having held the position previously?

Sir Paul Kennedy: Yes. I held the position for six years from 2006 to 2012.

Mr Winnick: Then you resigned or retired or whatever.

Sir Paul Kennedy: It is actually a three-year appointment, renewable, appointed by the Prime Minister. My second term of office came to the end and I did not seek to have a third one, nor would I have thought it appropriate, so I expired, if I can put it that way. Unfortunately my successor had a very serious road traffic accident and I was asked if I would step in for the time being, largely to see if he can come back, how he recovers. I am not intending, nor do I expect the Prime Minister to ask me, to stay on permanently. This is only a matter of months.

Q18 Mr Winnick: That is a matter for you. You have clarified the position entirely. As I understand it, you have written to all chief constables and directed them to provide you with full details of investigations that have used part 1, chapter 2 of RIPA, which are powers to acquire communication data to identify journalistic sources. What made you do that?

Sir Paul Kennedy: It started with the data retention decision in the European Court really. We have prepared a timeline that I think has gone on the website today, which gives precisely the background to what happened. The Government here reacted to that decision and then in September news was coming out about what was alleged to be misuse of powers in Operation Alice and also subsequently further allegations of misuse in the other operation, the name of which has suddenly escaped my mind, and those appeared in the paper. It seemed to us—

Chair: I think that was the Chris Huhne case.

Sir Paul Kennedy: Yes, the Chris Huhne case. One is Solar and the other is Alice.

Q19 Mr Winnick: On that particular case, Sir Paul, the paper concerned, *The Daily Mail*, claims the police were using anti-terrorism powers to spy on its sister paper, *The Mail on Sunday*, over the Huhne case.

Sir Paul Kennedy: May I come in on that? One of the things that has irritated me, and I have no doubt my successor, is the words "anti-terrorism". That is not what the Act says. It is, of course, used for that purpose, and rightly, but it is also for criminal investigations and for finding people who have been kidnapped or are about to commit suicide. It has all sorts of other uses.

Q20 Mr Winnick: Would you put the Chris Huhne case in that category?

Sir Paul Kennedy: I don't know and I am not going to be drawn, if I may be forgiven for saying so, into speculating about what the answers to the inquiries will show. But there was undoubtedly a crime there somehow because somebody, if I remember rightly, has been convicted of it.

Q21 Mr Winnick: You have told the Committee that RIPA is not simply a matter of dealing with anti-terrorism but also serious criminality, and of course whether this particular case—

Sir Paul Kennedy: At different levels—serious criminality in relation to interception, yes, but almost all criminality in relation to the use of data.

Q22 Mr Winnick: The media are sensitive, as they should be, to any abuse of power and our job, with other Committees in this House, is to try to identify whether there is any truth in the allegations being made. But the allegation is often made that RIPA is being used by the police in a manner that is not appropriate to the legislation.

Sir Paul Kennedy: That is not what we find, and we inspect a great deal of their work. What they are doing is using powers that are there to be used. I have taken this example before. Some of them are very important. Fly tipping a couple of years ago was the subject of a lot of media attention. The victims, you or I, don't like it if somebody has poured rubbish on our doorstep. One of the things you can find out by the use of RIPA is who did it, because sometimes the person who did it has used a card to persuade the person wanting rid of the rubbish which mobile to ring and the very starting point of a local authority investigation, not a police one, is that they need to know who that mobile belongs to, what in previous days we would have done by looking it up in a telephone directory. You can't do it, but you can do it by getting subscriber information under part 2.

Q23 Mr Winnick: Sir Paul, you give the impression—and that is your view and obviously we note it accordingly—that all is well.

Sir Paul Kennedy: No. I don't think that is the right way to look at these things.

Mr Winnick: If all is not well with RIPA, what is wrong then?

Sir Paul Kennedy: The whole purpose of an inspectorate is to keep watching to see what is going wrong. Last year we made something like 350 recommendations as a result of inspections. We are there to keep people up to scratch and to find when they do go wrong. I will take a random example. Sometimes a police supervising officer of the wrong level has given the authority for a particular type of inquiry. That needs to not happen and we try to make it not happen.

Q24 Mr Winnick: When do you expect replies to arrive from the letter that you have written to chief constables?

Sir Paul Kennedy: We have had extremely good replies. It is very dangerous to say all of the replies. We have had them all in but we now have to work on them, because it is not simply a one-line answer. We have three inspectors of my nine at the moment dealing with the responses we have received. As far as we can see, we have had full co-operation. Not surprisingly, some police forces, for example the Metropolitan Police, have a much bigger role than others and questions will have to be asked by us before we can evaluate what we have received. Does that answer?

Mr Winnick: Thank you.

Q25 Chair: You are saying you have had replies from the chief constables and they have given you facts and information, not just commentaries but actual numbers of warrants that they have issued?

Sir Paul Kennedy: They have given numbers, yes. I can go that far without trespassing.

Q26 Chair: Have you received any concerns about the way in which the police have tried to obtain the details of journalists?

Sir Paul Kennedy: The letter was directed to that.

Q27 Chair: You have not received any concerns yourself? Nobody has written to you?

Sir Paul Kennedy: What, journalists have written to me?

Chair: Yes.

Sir Paul Kennedy: Not personally, no, but on the other hand we made it clear in what we said that we are alive to the fact that journalists need to protect their sources. One of the functions of the Commissioner is to strike a balance. We are not there to be another voice for government or for the police service. We are there to see that the proper procedures have been followed.

Q28 Michael Ellis: Sir Paul, first of all can I commend you for your long public service, especially in view of what the Chairman has said about you stepping in.

Sir Paul Kennedy: Thank you very much.

Michael Ellis: You mentioned before about errors and you are conscious of seeing where errors have been made by the applying authorities and the like. Can you expand on what errors you have found, an example of the sort of errors you have found in your inspectorate?

Sir Paul Kennedy: Where have people gone wrong? One of the most common ways of going wrong on the data side in particular is in relation to transposition of numbers. That may sound a very small error, and in one sense it is. It may happen at any level. It may come from an informer initially and it may be progressed up the line, but it is an error. In the vast majority of cases it does not cause any problem at all because, for example, there is no such number. But in some cases it is catastrophic. If you have had time to read last year's annual report, you will have seen that on a couple of occasions police actually raided an innocent person's house on the basis of information that was never intended to be related to that house.

Q29 Michael Ellis: What was the consequence of that?

Sir Paul Kennedy: For the householder, appalling.

Michael Ellis: Did compensation follow to that householder?

Sir Paul Kennedy: I do not know whether any proceedings have been started or not. I don't even know what the framework is.

Q30 Michael Ellis: That was a simple error of someone typing in the wrong phone number, getting a digit wrong or something like that. Is there not a case for perhaps having to put the phone number in twice, as we ask people to put their e-mail address in twice and things of that sort?

Sir Paul Kennedy: Every time anything of that sort happens, there will be a report in relation to it and the need of the service, and of us as inspectors, is to try to make sure that some safeguard is in place.

Q31 Michael Ellis: Have you seen any examples of bad faith, for example the application of a warrant or otherwise deliberately to the wrong person or where suspicions have been aroused? I am conscious of cases where serving police officers have been alleged to have misused the police national computer in order to see what their ex-girlfriend or somebody else in whom they have a personal interest is doing. It would stand to reason that there may be some examples of people who would wish to misuse the powers that you have a responsibility to oversee. Have you seen any examples of that?

Sir Paul Kennedy: I can quite understand the question, but as soon as you think about it you realise that it is much easier, if you are a person who is authorised, to go on the police national computer than it is to obtain a warrant. Obtaining a warrant in bad faith is—I should never say impossible. I was almost tempted to say impossible, but you do have to go through an awful lot of stages. One of the seven or so people who has to handle it before it gets to the Secretary of State would be likely to flush out that this was not really genuine.

On the other side, data are not quite so difficult but even then safeguards are built in. For example, it is the normal practice in a police force that if they are conducting an investigation the person who gives the necessary authority to obtain the data from the service provider is not himself or herself connected with that inquiry. It has to be a senior officer who is separate from it. That can cause a little bit of a problem in a small local authority, not a police force, where the only people in trading standards who would know anything about it are three in number. But forgetting that, the answer to your question, have I ever seen it, I can only recall one and it was flushed out before it ever got as far as action. I think it was a postal worker who was trying to recover a package that she sent off by mistake or changed her mind as to whether she should have sent it off. It did not work, and in a sense that is slightly concerning because it was the only sort of bad faith one I can think of.

Q32 Michael Ellis: Can I ask you about something that is called the Wilson doctrine? What is that? What do you understand that to mean?

Sir Paul Kennedy: I sounded out about this in my annual reports a number of times. I don't want to be drawn into how much real teeth it has but I strongly feel that it ought to be abrogated. It was an undertaking given 40-odd years ago that Members of this House, and for that matter Parliament as a whole, would not be subject to any form of intercept, full stop.

Q33 Michael Ellis: Does it still apply?

Sir Paul Kennedy: I would like to say no, but I don't think anyone has tested the limits. I am conscious of the case of Mr Khan where he was visiting a prison to see, I think, a constituent. It was complicated because he was elected after he came under scrutiny and Sir Christopher Rose found that the prison who were doing the listening in were unaware of his different status. I can't

pretend that nobody has ever been listened to and this is why, for the protection of all of you, I would hate to think that you were a special category.

Q34 Michael Ellis: Just closing on that point, the pertinence of the question is, is there a procedure in place whereby you or someone in authority can check who it is that is being monitored and therefore be able to draw out from the system an inappropriate application? How would anyone know that it is not appropriate to intercept communications from a named individual?

Sir Paul Kennedy: You don't always know the name, you are quite right. Very often you don't because the information you get is a telephone number or an address or something of that kind, so you can't always draw it out.

Michael Ellis: So it might be missed?

Sir Paul Kennedy: Yes.

Q35 Chair: Have you come across many mistakes? There is a view by some that the number of mistakes was quite high.

Sir Paul Kennedy: A mistake is an error really, whichever way you look at it.

Chair: Yes, a mistake is an error. I think we can agree on that.

Sir Paul Kennedy: It is a question of whether you are targeting the wrong person or whether you have simply made an error mechanically in what you were doing.

Q36 Chair: Have you come across many mistakes or errors?

Sir Paul Kennedy: The numbers are in the report. One is too many, but in real life you are always going to get some transposition errors. There are problems about all of these things. With transposition errors, for example, if you mechanised the system you eliminate my telling you but, on the other hand, if I get it down wrong in the first place and commit it to machinery it propagates it.

Chair: Very helpful.

Q37 Dr Huppert: There are so many things I would love to pick on, but I am not sure we quite finished off on Mr Ellis's question about the Wilson doctrine. I am interested, not specifically because I am particularly interested in how parliamentarians are concerned, but I think it raises questions about the level of scrutiny of individuals being looked at. Who would know if there was interception on a parliamentarian, a lawyer, a journalist? Would you or your role necessarily know that? Would anybody be able to verify that or are we relying on the Secretary of State just getting it right?

Sir Paul Kennedy: If the Secretary of State were minded to sign a warrant to listen to your communications, she would know that it was you, because at that stage the target is identified, but in many cases the target is not identified. Sometimes certain types of warrants are drawn in broad terms, for example people coming to attend a meeting of Al-Qaeda at a Westminster hotel.

It is unlikely that there is such a meeting but supposing there were, it could well be the subject of a warrant and at that stage the names of the individuals would not be known.

Q38 Dr Huppert: Nobody would ever be able to verify whether the Wilson doctrine was being applied, whether any code of conduct on journalists or lawyers was being applied?

Sir Paul Kennedy: I am not involved in it but I am told that there is an ongoing case before the tribunal that involves some aspect of the Wilson doctrine. I can't say any more, but that is sufficient to answer your question. The other thing in any event, of course, is that section 19 has its own problems because it is the one that forbids general discussion of anything that has come up naturally in the course of this type of work.

Q39 Dr Huppert: That is indeed a challenge as to how we make sure that the checks are being done correctly. I am fascinated because you said you have a lot of information from police officers. We did not get a chunk of information when we asked, because they said a lot of it was secret information that was being sent to you about interception. We were also told a huge amount of information was not routinely recorded.

Sir Paul Kennedy: Can I just help you with that? I have a power—and there is no reason why you should be aware of it—in section 58(1) that is very wide indeed, “Co-operation with and reports by a section 57 commissioner”. It shall be the duty of a whole list of people, one of whom is every person holding office under the Crown, “To disclose or provide to the Interception of Communications Commissioner all such documents and information as he may require for the purpose of enabling him to carry out his functions”. I have a statutory power to get it.

Q40 Dr Huppert: I understand that, but we were told that we could not be provided with some information because it was secret. On others, such as data relating to the profession of the subject of investigation, it is not routinely recorded. I am interested that they are giving you information on access to journalists and they are telling us that they do not have that information, which is different from saying they can't send it to us. Are you getting complete answers to all of your questions?

Sir Paul Kennedy: If you have had answers you think we ought to see for the purpose of our inquiry, we would be delighted to see them.

Chair: Excellent. We will send it to you. Dr Huppert is absolutely right that in a number of cases we have been told that the information is not even held, so we will certainly be sending it to you.

Sir Paul Kennedy: I am not going to comment. I have no idea whether or not it is the same information.

Chair: No. We will send it to you.

Q41 Dr Huppert: One last question on a similar area. We could talk a lot about errors and incorrect data and various other things in the report. I have been interested in the Telecommunications Act 1984, section 94, that gives very broad powers. In your experience, when you had the job previously and now, have you ever had a chance to look at how it is used, whether it is used proportionately, or are you aware of anybody who does?

Sir Paul Kennedy: I think as far as I am concerned that is off limits because it is not part of my remit at all. I am only concerned with RIPA.

Q42 Dr Huppert: Are you aware of anybody at all who has ever looked at it?

Sir Paul Kennedy: I am sure it has been but not me, is all I can really say.

Dr Huppert: That is what everybody says.

Sir Paul Kennedy: I agree.

Q43 Mr Clappison: I am sure many people will be heartened to hear of your concern for proper protection for journalistic sources. The question just occurred to me—

Sir Paul Kennedy: Of course and, if I may say, for others too. It also goes for doctors and, dare I say it, for lawyers.

Mr Clappison: Perhaps we will just stick to journalists. Have you seen cases where you have thought that the powers have not been used properly in relation to journalists and their sources?

Sir Paul Kennedy: I am not conscious of ever having seen a case where a journalist was the subject of, for example, a warrant. I am not going to say that there have not been cases where journalists have been in the target area of an investigation, and there is an obvious difference. I think it would be improperly used if the journalist was the subject of the warrant and there was no justification for the journalist being the subject of the warrant, but sadly journalists, like lawyers, can sometimes put themselves in a position where they ought to be the subject of a warrant.

Q44 Mr Clappison: I understand that. If I can ask you one other question arising from that: would you be prepared to share with us any thoughts as to how you think journalists and journalist sources could be appropriately protected in future?

Sir Paul Kennedy: There is nothing in here. That is the Acquisition and Disclosure of Communications Data Code and there is nothing in that in relation to how to deal with journalistic material. Presumably you are talking about sources rather than the individuals?

Mr Clappison: Yes.

Sir Paul Kennedy: However, there is in the code that governs intercept. The Home Office is well aware of this. They have said that they are preparing a draft new code, partly starting from what happened in Europe. We have encouraged them to expedite it so far as possible, because the code should contain special provisions for dealing with that kind of material. Does that answer?

Mr Clappison: Thank you very much.

Q45 Chair: You are happy with the fact that the code may be amended? You think that is a way round it?

Sir Paul Kennedy: It ought to be.

Q46 Nicola Blackwood: Sir Paul, I just wanted to go back on a couple of points that you have made. Regarding Operations Alice and Solar and accepting the fact that these are all allegations, as I understand it the allegations are that police accessed logs that would be the access of data. They would require merely to pass the threshold of needing to be solving some sort of criminality. Is that correct?

Sir Paul Kennedy: There has to be criminality. I don't want to get drawn into the facts because I don't know enough about them and I think it is very important not to be.

Q47 Nicola Blackwood: It would therefore be legal. They would not have been doing anything illegal in that case. On that basis, and following on from what you have just been saying to Mr Clappison, as I understand it the draft code that you are referring to was drafted eight years ago and it has not been updated since then, has it?

Sir Paul Kennedy: No, that is right. It was done some years ago and it needs updating.

Q48 Nicola Blackwood: It does not contain any advice for professions that are dealing with privileged information.

Sir Paul Kennedy: Yes. As I said, the warrantry code does deal with professions and privileged information in a reasonably adequate way. The data one does not.

Q49 Nicola Blackwood: That would include Members of Parliament, helplines and all sorts of sensitive information?

Sir Paul Kennedy: Yes.

Q50 Nicola Blackwood: What sort of advice would you like to see the Home Office including in terms of improved consideration when it comes to the level of intrusion you are thinking about, where it comes to data in particular in addition to interception?

Sir Paul Kennedy: First of all, one has to remember that data do not normally involve content at all.

Nicola Blackwood: It would if you were in an MP's office and you are talking about a constituent contacting you regarding a very sensitive case.

Sir Paul Kennedy: That is why I put in the word "normally". If you are in regular contact with a cancer specialist, it may be reasonably inferred you have some problem but it does not actually intrude in the same sort of way. What I would like to happen, and I am sure will happen—and in a sense I do not want to answer your question—is I want to see what the journalists say about the protection they need and what the police service says as to what they need in order to do their job.

Q51 Nicola Blackwood: What sort of mechanisms would be practically workable?

Sir Paul Kennedy: If you are talking about data, I think the trouble is that initially you very often don't know that you are targeting somebody who may not wish to be targeted as a journalist, because you are gathering up information to relation to telephone numbers or areas or whatever. But once it emerges that it is so, as happens in relation to warrantry, it should be drawn to my attention, and it is in relation to warrantry.

Q52 Nicola Blackwood: Can we talk about that? In your answer, I think it was to Dr Huppert—

Sir Paul Kennedy: Not at the permission granting stage. I am an auditor afterwards.

Nicola Blackwood: I understand that. We were talking a little bit about compliance and you were saying that as far as you are aware there are no cases of lack of compliance, but you are also saying that you don't know who is being targeted.

Sir Paul Kennedy: Not always, no.

Nicola Blackwood: Not always. What we are talking about at the moment is the difference in targeting individuals who hold sensitive data and the consequences that may follow. As I understand it, under section 8 of the Act there are two different kinds of warrants. There are subsections 1(a) and (b) that require the person or set of premises to be intercepted to be named or described and then subsection 4 is the broader power. I know that that has the different protections under subsection 16, but nevertheless do you think that there are changes that could be made within that section that would address the problem that you are identifying as the auditor? If the auditor is unable to distinguish in his audit trail between those who have sensitive information and those who don't then we are never going to resolve the problem.

Sir Paul Kennedy: We are able to distinguish if the information is available by the time the audit comes along. There is no difficulty.

Q53 Nicola Blackwood: But what you are saying is that it is not always.

Sir Paul Kennedy: It is not always.

Nicola Blackwood: How can we resolve that?

Sir Paul Kennedy: A journalist may be targeted by way of having his contacts investigated without anybody knowing that he or she is a journalist.

Q54 Nicola Blackwood: Yes, but where it is known, how can we resolve this and make sure that we do know that we are protecting journalistic sources, excluding situations where—and I hope we are not—we are targeting the whole of SW1?

Sir Paul Kennedy: I don't see how you can protect people if you don't have the basic information and I don't see that there is any way in which one can get that information at an earlier stage in an investigation if it is simply not there.

Q55 Nicola Blackwood: You don't believe that when the police put in a warrant to the Home Office—

Sir Paul Kennedy: A warrant?

Nicola Blackwood: When they are making an application for data they are not—

Sir Paul Kennedy: I am sorry to chip in but it is so important to keep the two separate.

Nicola Blackwood: Yes. When they are making an application for data they are not able to distinguish between whether they are targeting someone who is holding privileged information or not and you don't think that there should be some kind of mechanism that they should be making that distinction?

Sir Paul Kennedy: Forgive me, it does not work like that.

Nicola Blackwood: How can we make it work?

Sir Paul Kennedy: If we take a London bombing, because I do know what went on in those sort of cases, you want to know who was using their mobile telephones within a radius of 100 yards at the time the thing went off. Nobody is going to tell you in advance that one of them was a journalist.

Q56 Nicola Blackwood: That is fine, but we are not targeting journalists in those cases. We are talking about cases that allegedly do target journalists and, with respect, I think we are slightly getting lost in the wood for the trees. In the case of Operation Alice and Operation Solar, allegedly *The Sun* and *The Mail on Sunday* were both specifically targeted in order to find out journalistic sources. In a case such as that—

Sir Paul Kennedy: Quite soon I will publish a report in relation to those. I am not going to speculate about them at the moment.

Q57 Chair: Sir Paul, Ms Blackwood is not asking you to speculate. She is just using them as examples to make the point to you.

Sir Paul Kennedy: Yes, but I think concrete examples of that kind are unhelpful, given the nature of the inquiry going on.

Chair: It is the only example she has.

Nicola Blackwood: What I am trying to ask is what sort of improvement to our current regime could be put in place to make sure that we do not have a recurrence of such a similar hypothetical situation? What sort of improvement could be put in place so that you as auditor would be able to distinguish between data applications for the general public and for those who are handling sensitive information?

Sir Paul Kennedy: Let's understand this. If you know that you are seeking data in relation to a professional, a journalist or a lawyer acting for a defendant, then you still have to ask a lot of very important questions under the Act. You have to ask about proportionality, whether it is necessary, whether there are any other ways of getting the information you seek, if the information is purely relating to crime. I think that has to be emphasised in the code when it is revised.

Chair: That is very helpful. Thank you. We will reflect on what you have said.

Q58 Dr Huppert: You talked about very broad warrants and a lot of people being brought into those, and you gave an example of asking for everybody within 100 yards of a phone mast. Can you give us a sense of what the broadest warrants are that you have been made aware of, in terms of the area covered and the number of people that could be in one warrant?

Sir Paul Kennedy: I would have to go back to them, because it is a couple of years ago, and I am not going to say more than this but I think it may be helpful to you nevertheless. There were one or two quite wide warrants in the run-up to the Olympics.

Dr Huppert: Quite wide? It would be helpful to have some sense in terms of what one warrant looked like.

Sir Paul Kennedy: Sometimes they were wider in relation to people and sometimes they were wider in relation to area.

Dr Huppert: City-size wide; 100 yards wide?

Sir Paul Kennedy: Not city-size wide but a certain geographical area. I don't think we can give any examples, can we? I think the trouble is, apart from anything else, we have section 19 over our shoulder.

Q59 Dr Huppert: Part of the problem is how we can know what the import of one warrant is. You are looking at 10% of them, but if one warrant happens to cover an entire borough it is obviously rather more important.

Sir Paul Kennedy: May I assure you that any significantly wide ones were always inspected personally by the Commissioner in my time and I am sure they still are.

Q60 Dr Huppert: Would you be certain that that always happened?

Sir Paul Kennedy: Yes.

Q61 Paul Flynn: In one of your answers you said that on the question of protecting the sources of journalists you took a balanced view, and that implies that you think that the right of journalists to have their sources protected is sacrosanct in some circumstances. In what circumstances are they not sacrosanct and they are allowed to be breached?

Sir Paul Kennedy: When they are thought to be a first-stage partner to a crime, if they are conspiring with somebody to do something. It does happen occasionally.

Q62 Paul Flynn: Is that your experience in the cases that you have had?

Sir Paul Kennedy: Yes. Not many.

Q63 Paul Flynn: There have been some enquiries by *Press Gazette* asking for details under Freedom of Information of the number of warrants that were issued and so on, the number of times they are going, and they have never been given information, sometimes refused on the grounds of national security and sometimes on the grounds of cost. Is there anything sinister in this lack of information?

Sir Paul Kennedy: Being refused by—?

Paul Flynn: By the police forces. I believe they applied to every police force in the country for details under Freedom of Information and they did not get a positive response from any of them.

Sir Paul Kennedy: I think you would have to look at the individual cases. I would not want to generalise across the board. I can well envisage cases where it would be wholly inappropriate to give the information and others where I would have expected it to be given.

Q64 Paul Flynn: What would they be? What are the ones where you would expect it to be given?

Sir Paul Kennedy: If there is no true national security element involved in it.

Q65 Paul Flynn: When will your report be published?

Sir Paul Kennedy: Having not finished the investigation, that is a very dangerous question to try to answer. We hope to be able to finish the investigation within the calendar year, in other words within the next couple of months, depending on what—when you get answers, they generate questions and you then ask the questions and see where that leads you. We are talking about within the next few months.

Q66 Paul Flynn: Do you expect that as a result of your report there will be action taken that will quell the fears that many people have about the present system?

Sir Paul Kennedy: I am never so optimistic. I think people will know better what happened.

Q67 Chair: As well as doing that report, you are also finishing a report to the Prime Minister. Is that right?

Sir Paul Kennedy: Yes.

Chair: What is that on?

Sir Paul Kennedy: The report to the Prime Minister is that report. We promised to render it to the Prime Minister. The extent to which he decides to publish it is, as always, a matter for him, but it goes first to him.

Q68 Chair: Of course. We would not want to presume as to what is in the Prime Minister's mind. We will leave that up to him. Your timetable changed slightly. You said that you hoped that this would be completed by the end of the calendar year. Is that when you think you will hand the piece of paper over to the Prime Minister?

Sir Paul Kennedy: No. We are much more honest than that. I hope the work will have been done to produce the report. It will then have to be written and processed and these things take time, but that is the sort of timescale we are looking at.

Q69 Chair: Of course. I realise that a lot depends on the length of the report and who writes it, and possibly even the state of the weather, but do we have a precise date when you would like to have a hard copy in your hand to give to the Prime Minister, maybe the end of January, February, March, next year?

Sir Paul Kennedy: Can I ask the lady sitting behind me what she thinks?

Chair: You can ask anyone in the audience that you like, Sir Paul.

Sir Paul Kennedy: She says by the end of the year. I don't believe her, to be honest. I think January is better.

Q70 Chair: You don't believe your own chief of staff? Your chief of staff is telling us that it will be done by the end of the year but you don't believe her. It sounds a little vague, Sir Paul, about something that is really important. These are very serious matters.

Sir Paul Kennedy: It isn't that the information is not there, but what has happened is that the responses we have had so far, which have been very co-operative—

Chair: No, I understand that, but this is a Committee of the House. We are doing an investigation. When we do our reports we don't absolutely know the moment that we are going to publish, but your chief of staff has told you that this is going to be ready by the end of the year. Is that your understanding or do you think it will be later?

Sir Paul Kennedy: That is when I think the information will be ready to be written up. I don't think one should set deadlines that are unrealistic and then have to move them.

Q71 Chair: I think the Committee would like a deadline set. We would like to know because it can't—

Sir Paul Kennedy: 31 January.

Chair: 31 January. That is very helpful. It took some time but we—

Sir Paul Kennedy: It may be moved, but 31 January today.

Chair: We are delighted, Sir Paul. We now realise if we had had all day it could have possibly even been 1 January. Excellent. We are most grateful. Thank you very much.

As you say, when you ask questions further questions come forward and certainly your evidence today has given us many more questions. Thank you very much for coming. We are most grateful.

Sir Paul Kennedy: Thank you very much for your attention.

Examination of Witness

Witness: **Michelle Stanistreet**, General Secretary, National Union of Journalists, gave evidence.

Q72 Chair: Good afternoon, Ms Stanistreet. Thank you very much for coming to give evidence to this Committee. The Committee is having a look and we are going to produce a short report by the end of November on the subject of RIPA. The NUJ has concerns. You have stated, “The misuse of RIPA to snoop on journalists is not an isolated example of bad practice in the Met. The police clearly believe that they are above the law they are there to uphold”. Do you believe that the, as you put it, snooping on journalists is widespread and why do you think this is happening?

Michelle Stanistreet: One of the problems is that we don’t know just how widespread it is. The revelations that this has even happened only came about as a result of journalists realising it in the Met’s report on the so-called Plebgate affair. It was a throwaway line about the accessing of a political editor’s phone records in this way. We had no idea that this was taking place and it is only through the dogged journalism that has happened since that some examples of this happening have come to light. We believe it is only the tip of the iceberg. One of the problems is that the individual police forces who have been approached with Freedom of Information requests have been stalling and claiming that for cost reasons and time purposes they can’t provide answers. So many examples have been revealed in recent weeks that we believe this has been pretty much systemic and institutionalised, and it has not just happened in one police force. It has clearly been happening among many different police forces.

Q73 Chair: We will come on to the Freedom of Information requests by *Press Gazette* in a moment, but just in respect of the possible damage that this might do to the reputation of the profession, do you think it will cause damage to the public’s trust in dealing with journalists?

Michelle Stanistreet: I think the revelations as they stand have already had a major impact and have sent shockwaves through the journalistic industry. Journalists live and die by their sources. We ask people to come to us and we promise, we pledge to protect their confidentiality, their anonymity. It is often very brave people who take a decision that the information they are in receipt of should be placed before the public, and journalists are the route to do that. The knowledge that their identities and information about them has been accessed secretly in this way has done irreparable damage. We might not see the impact of this for many years, but without that relationship of trust between journalists and potential sources and whistleblowers the impact on journalism is potentially immense, and to investigative journalism particularly.

Q74 Chair: Do you think that this is an attempt to target individual journalists and newspapers, or do you think it is just something that has progressed because of the numbers of warrants that have been issued and if you go for a larger number then it is inevitable that you will find a journalist? We have just had evidence from the Interception Commissioner and he basically said to this Committee that sometimes these warrants are taken out and you don’t know it is a journalist. You check numbers, you are given a number, and at the end of the day you discover it is a journalist and then you destroy the information. Do you think it is something that is targeted or do you think it might just be accidental?

Michelle Stanistreet: It is quite clearly being targeted because in some of the cases that have already come to light individual journalists were targeted specifically because they had reported

on these events. The police seem to be much more concerned about identifying what they might see as potential disloyal leakers in their own organisations and institutions than they have been about the damage being done to journalism and the relationship of trust between whistle-blowers and journalists. It is quite clear there are a number of examples where I think police have taken a decision to waste public money and resources on snooping on journalists in local newspapers, as well as in national newspapers, rather than concentrating on the many crimes that are out there to investigate.

Q75 Chair: You think it is happening. You don't know the extent, but you would like it stopped?

Michelle Stanistreet: There have been a number of absolute cases where it has been clearly shown that different police forces have admitted that they have been doing this, but what we do not know is the scale of it. One of the problems is that they are not even logging information about the occupations of the people that they are snooping on.

Q76 Chair: Do you think they should? Do you think when a warrant is issued the occupation—should it just be the occupation or should it be other issues?

Michelle Stanistreet: They simply should not be doing it in the first place. This piece of legislation was never envisaged as a means of snooping on journalists and preventing journalism from thriving and flourishing. So it should not be happening in the first place. There should be transparency. The NUJ have campaigned a lot in recent years about what we have seen as the growing trend of the police using journalists and the information we gather in the course of our work and photographs that are taken as a shortcut to their investigations. It is vital that journalists are not seen as an extension, an instrument of the police or the state in that way. It comprises the ability for journalists to do their job independently and to be seen to do that fairly.

Q77 Tim Loughton: Could we come back to *Press Gazette's* FOI that the Chairman referred to just now, which revealed that the Met does not keep records of monitoring cases of RIPA against journalists? I think you said that it is the tip the iceberg. How many cases are you aware of and how extensive is it?

Michelle Stanistreet: We know that there has been something like 54. I could double check that for you. There have been a number of reports about specific cases and a number of journalists who are trying to establish, as we speak, whether they have been investigated and their sources comprised in this way. It is a very rapidly moving story in this sense. The diversity of instances where this piece of legislation has been used is revealing enough. There have been cases where councils believe that there have been leaks about their business where they have obtained permission for a journalist, sitting in a coffee shop, meeting with potential sources and witnesses, to be covertly watched and their movements monitored. It is beyond ludicrous that this has been allowed to take place without any kind of assessment or transparency about doing it and with the journalist, and more critically their sources and whistle-blowers, none the wiser. It is an outrage that it has taken place.

Tim Loughton: You think it is a pretty big iceberg.

Michelle Stanistreet: I believe so.

Q78 Tim Loughton: You used the term systemic and institutionalised. Define systemic. Is this something where they get together and discuss how they can do it in different parts of the country, or what is it?

Michelle Stanistreet: Who knows? The first example that came to light was within the Metropolitan Police, but it is quite clearly not a problem that is confined to the Met, so it goes beyond one individual police force. There are many others, such as Kent, that have been implicated in the examples that have been revealed to date. We believe that there is such a geographic spread that it shows that many police forces, whether individually or somehow collectively, cottoned on to the fact that they could exploit this piece of legislation in this way. It was certainly never conceived of as being a mechanism to access journalistic material when it was first brought into being. I think the former Met chief, Ian Blair himself, concedes that if this had been anticipated as a potential consequence, it would never have been passed in the first place.

Q79 Tim Loughton: Do you think there are police forces that are “safer” or are you just not aware of that?

Michelle Stanistreet: I would very much doubt so, but it does not really matter whether it is every single police force doing it or whether just some are. The very fact that it has been brought to light now and there is public exposure about the fact that they can do this legitimately, it seems, would presumably, without any move to clamp down on this, mean that many more police forces would do it.

Q80 Tim Loughton: My point is that the fact that they apparently can on the basis of the high profile cases in London, Kent and others does not mean that they are all actually doing it and some police may have taken a much more cautionary approach so as not to become the subject of such allegations?

Michelle Stanistreet: You may find that out in the course of your investigation, but I don’t think that is particularly relevant. The fact that it is happening and on a broad scale is shocking and incredibly undermining of journalists. When whistleblowers are making a huge decision and wrestling with themselves about whether they should bring forward information into the public domain, I don’t think they should have to go through the process of trying to establish whether their local police force is more honourable than another local police force.

Q81 Tim Loughton: I am trying to establish whether there is a bad cop, good cop situation. You are suggesting to me it is all bad cop, bad cop.

Michelle Stanistreet: No, I didn’t say that. I said it is a problem that is quite clearly widespread; the facts speak for themselves. We shouldn’t be down to the position where journalism in the UK is dependent on whether there is a bad cop, good cop. In actual fact, the police are doing stuff that they can do within the law as it currently stands. It is wrong and it should never have been allowed to become established in this way. I am sure you will have witnesses from the police who

absolutely defend their right to do it. I would wholeheartedly disagree with that, but frankly I don't care about one superintendent's perspective on press freedom or the way journalists do their jobs or the vital role of whistleblowers in our society. It is a much more important issue than one superintendent ticking a box and filling in a form or one particular police force's approach to the critical role that journalism plays in society.

Q82 Chair: It is not a big ask, is it, to write down the profession of those that you are getting warrants for?

Michelle Stanistreet: You wouldn't have thought so, but clearly it has been beyond the bureaucratic processes of some police forces, or so they claim. I think this is something that they should not be allowed to hide in bureaucracy. They should be forced to deliver up the information.

Q83 Dr Huppert: Many of us have campaigned for a long time on transparency in this whole space, so we know what is being done and how much of it is reasonable and how much of it is not. As I am sure you know, there are seven grounds on which communications data can be collected: national security, prevention of serious crime, disorder and a few others. Do you know which ones have been used to collect information on journalists?

Michelle Stanistreet: I would have to double check that for you, but the nature of the cases have been quite diverse. There seems to be a pattern in the police trying to investigate what they would see as their own bad apples who have leaked information to the press in some way. That seems to have been the overriding motivation for doing this.

Q84 Dr Huppert: It would be helpful, because there are seven clear reasons and I don't see one of them being police leaking.

Michelle Stanistreet: No. I would have to double check what they have cited.

Dr Huppert: It would be very helpful to understand how they have tried to crowbar it into what Parliament decided were the things. National security is one thing and police officers talking out of turn is not the same thing at all.

Michelle Stanistreet: It is absolutely not.

Q85 Dr Huppert: If you do have any information on that, it would be very helpful for us to look at it. You asked for the Interception of Communications Commissioner to do an investigation into this. Do you have confidence in his inquiry?

Michelle Stanistreet: We called for an inquiry, so we are pleased that an inquiry is taking place and we will contribute to it fully.

Dr Huppert: That is not quite the question I asked.

Michelle Stanistreet: I think the reality is that it would be very easy for an inquiry to take place and then there to be some tweaking of a code as the final outcome of it. The NUJ does not

believe that that is good enough; it would not go far enough. What is so important in the course of his inquiry is that we get to grips with the extent of what has been happening under this piece of legislation, the full scale, the extent and the real detail of the cases that have been pursued. I think the outcome of this investigation is the most important thing and we have concerns that it will not go far enough.

Dr Huppert: You have not quite answered whether you have confidence in the inquiry, I notice.

Michelle Stanistreet: We called for an inquiry. Until it has taken place and come to an outcome, I think it would be unfair to assume it is lacking in integrity.

Q86 Dr Huppert: What you would like to see is a clear analysis of how much of this has happened—so what has happened, how it has fitted in—but what else do you wish to see? Presumably you could not have a system that said that anybody who is a journalist is completely excluded from anything, if they are genuinely involved with a terrorism plot for example. What would you like it to actually say?

Michelle Stanistreet: The legislation was never brought in to deal with terrorism in that sense and journalists are obviously not terrorists.

Q87 Dr Huppert: Essentially it was specifically brought in to try to deal with things like terrorism. National security is the first on the list. What I am saying is that it is possible for somebody who is a journalist or a lawyer to also be involved in serious criminality, separate from their role as a journalist.

Michelle Stanistreet: Perhaps we will see in the course of this investigation whether there has been any example where that has happened. I very much doubt that that is the case.

In terms of what we would like, there are already existing pieces of legislation in place, hoops that journalists have to go through if the police wish to serve a production order, the provisions within PACE for the protection of journalistic material, which is protected under European legislation. The NUJ has defended many of them and many individual members of the NUJ when they or a newspaper group have been served a production order. They are very stressful, difficult and expensive but at least they happen in the full glare of transparency, through a legal process and mechanism, and a judge takes a decision at the end of the day. At the moment what we have is a system whereby police superintendents can take that decision based on their own internal issues and interests rather than the broader ones of journalism. Journalistic material should be privileged and protected.

Q88 Dr Huppert: I am trying to be clear about what you are asking for. Are you saying that anybody who is a journalist should be completely excluded from this legislation? Are you saying that all use of this legislation should be subject to judicial oversight? What exactly are you asking for?

Michelle Stanistreet: At the very least there should be judicial oversight.

Dr Huppert: For everybody or only for journalists?

Michelle Stanistreet: Journalistic material should not be allowed to be accessed without judicial oversight. The consequences of allowing what has been happening over recent years to carry on is incalculable for journalists.

Q89 Chair: It is not just the system we have at the moment, the auditor after the event, which is what we have with the—

Michelle Stanistreet: No.

Chair: You want it as the process proceeds?

Michelle Stanistreet: Absolutely.

Q90 Chair: If you look at the number of investigations of Scotland Yard in relation to journalists, there are quite a lot. There is Weeting, Elveden, Pinetree, Golding, Sacha, Tuleta, Kalmyk, Sabinas, Carrizo—quite a lot.

Michelle Stanistreet: If the police want to access journalistic material and privileged source information they should transparently ask for it and go through a legal process and have the legal argument to assess whether it is an appropriate request or not. The journalists know about it, the sources know what is happening, the news groups know about it at the time, and that process can happen with full transparency and openness, not this backdoors route to get their hands on journalistic information secretly in the way that has been happening.

Chair: Thank you. I think we get the point.

Q91 Michael Ellis: Ms Stanistreet, if I could clarify a couple of things with you. The point that I think Dr Huppert was getting at is journalists are not above the law, in the same way that politicians are not above the law. Do you accept that? There must be a process whereby if there is due and proper cause for proceedings to be taken against journalists or politicians they can be taken. Do you accept that?

Michelle Stanistreet: Of course.

Michael Ellis: Sir Paul Kennedy was saying that the process as it currently stands means that they do not really ascertain the occupation of the person involved. He said it in relation to what is called the Wilson doctrine. They can't even determine whether someone is a politician or not within their processes at the moment. Do you accept that as an explanation for—

Michelle Stanistreet: No. It seems a pretty basic flaw in their processes in that case, doesn't it?

Q92 Michael Ellis: As far as the records are concerned, I understand police forces have been saying that because of the sheer volume of records in connection with metadata, for example, it would be prohibitively expensive for them to trawl through thousands of their records to ascertain who is and is not a journalist. Do you accept that as an explanation?

Michelle Stanistreet: I don't accept it as an explanation. Obviously it is one that they have proffered. It does not react in any way with any cognisance of the seriousness of what we are

doing. I think this is such a vital thing that I am afraid the expense involved, the bureaucratic difficulty is something that the police are going to have to contend with and do in order that the investigations taking place have all of that information at their fingertips.

Q93 Michael Ellis: Do you agree with me that the wrong legislation has been applied here, that what is called the RIPA proceedings are the wrong legislation for police to use in respect of journalists anyway? There are proper safeguards that are supposed to go through judicial oversight and if the police have used the RIPA legislation it was wrong in principle for them to do so.

Michelle Stanistreet: Absolutely. I believe it was a misuse of what that legislation was devised to do. There are safeguards in other pieces of legislation for journalistic material.

Q94 Michael Ellis: Do you think there has been a deliberate bypass of the safety procedures whereby a judge is supposed to be addressed with a particular issue concerning a journalist so that he or she can make an informed legal judgment as to whether it is appropriate and reasonable in all the circumstances for intercept to take place against a journalist? What they have done is used the RIPA legislation in order to bypass that judicial oversight because, quite frankly, they were scared a judge would say no.

Michelle Stanistreet: Absolutely. In some of the cases a judge has said no about revealing the identity of sources involved, so it is quite clear that there has been a bypassing in that way and that it has been deliberate and it has not been a one-off incident. It has happened many times.

Q95 Dr Huppert: I understand your desire to carve out an exception for journalists in much of this. How would you define a journalist?

Michelle Stanistreet: An individual who is engaged in news gathering. The NUJ has over 30,000 members of our union in the UK and Ireland who work in many different parts of the industry as journalists.

Q96 Dr Huppert: Would it include citizen journalists, people who report on local council meetings and say what is happening? How broad a line would you like to draw?

Michelle Stanistreet: It depends on the nature of their work. We have bloggers who are in NUJ membership. It could be devised in a way that reflects the trade union membership that individuals have, the places where they work, the places where they commission. We have freelance members in our membership. The very fact of journalism as being a diverse occupation and industry means that one person's citizen journalist is somebody else who is providing local news because their local newspaper has just closed down. It is very diverse industry.

Chair: Thank you. That is very helpful. We will also consult the Oxford Dictionary, or the Cambridge Dictionary in Mr Huppert's case, on what a journalist is.

Q97 Mr Winnick: You said and agreed that journalists should not be above the law, as indeed illustration was given that politicians are not above the law. Has it ever been suggested by the NUJ that journalists should be above the law?

Michelle Stanistreet: It has never been suggested that journalists are above the law and we operate within the law daily as journalists. There are many different pieces of legislation that cover journalistic activities in that sense.

Q98 Mr Winnick: There is a distinction, of course, when one talks about journalists being above the law, and you said that the union has never adopted that line, understandably, but do you take the view that the source of material that journalists receive should not be revealed under any circumstances?

Michelle Stanistreet: One of the overriding responsibilities of any journalist—and the NUJ has one of the oldest codes of conduct in the world—is to protect your sources. It is the fundamental tenet of what journalists stand for and journalists have very proudly defended that pledge over many years. We have fought legal cases that have lasted many years. The ability and right to protect your sources has been stripped away by the very existence of the activities that have been revealed in this way by *Press Gazette* and others. That is an incredibly disturbing thing because that is a central part of that relationship of trust between sources and journalists that has been undermined by what has been going on and by the reality, the news that it has been happening in this way for many years now.

Sorting that out and acting to halt that is critical if the public are going to have trust in journalists going forward. You can think of so many major inquiries and investigations and scandals that have been broken because of people being brave enough to come forward with information that journalists have revealed to the broader public, and it would stymie the ability of journalists to carry on doing that vital work in future if this is not halted.

Q99 Mr Winnick: It is true to say that journalists have gone to prison for refusing to reveal—

Michelle Stanistreet: Absolutely.

Mr Winnick: Mulholland is a name that comes to mind, that occurred many years ago.

Michelle Stanistreet: Yes, there have been a number of different cases of that and journalists have been held in contempt because they have stood up for their sources and protected their identities. It is important that we are allowed to continue to do that in the future. The existence of digital communications and the way in which journalists rely on them and information is passed on should not be used somehow as a backdoor route to finding and accessing material that can be used to identify sources who have trusted journalists.

Q100 Mr Winnick: The allegation has been made by *The Daily Mail* that its sister paper, *The Mail on Sunday*, was the subject of the police using anti-terrorism powers to spy on the newspaper over the Chris Huhne investigations. Do you have any comment on that?

Michelle Stanistreet: After *The Sun* example that sparked all of this off, it was one of the instances that came out soon after in the Chris Huhne speeding points scandal—so this is an issue about speeding points; it is not a matter of state or terrorism—that they secretly obtained the phone records of the journalist involved at *The Mail on Sunday*, David Dillon, and his source who was a freelance journalist.

Q101 Mr Winnick: Are you accepting as a union that this actually happened?

Michelle Stanistreet: We absolutely believe it happened. I think the evidence is there to demonstrate that it did and the police have accepted that, as they have many other cases: a journalist at the *Ipswich Star*, so the Suffolk police; a journalist in Derby who was spied on while she was meeting with her contacts. These things have been happening for a number of years. The police very swiftly after this legislation was introduced saw the opportunity it gave them to do this, which is why it is not one-off, it is not accidental, it is not happening to journalists incidentally, regardless of their occupation. Journalists and their sources have clearly been targeted in this way.

Q102 Mr Winnick: North Kent Police have stated, as what they describe as part of this debate, that in their view, "Consideration has to be given to how material held by the media that might be relevant to a criminal investigation is shared with the police and the courts". What are your comments on that?

Michelle Stanistreet: If they want to get hold of journalistic material they should be upfront about it and they should go through the existing procedures, whether they serve a production order, and there needs to be judicial oversight. It should not be down to one police superintendent who is carrying out an investigation to make up the rules on this and decide what should or should not be in his purloin. The journalist should know, the newspaper should know, the source should know, and there should be a legal argument about it.

Q103 Mr Winnick: If the police are of the view that this is essential to their investigation, instead of doing what apparently they have been doing, they should use the judicial process?

Michelle Stanistreet: Yes. They are using this piece of legislation as a secret means of getting their hands on something that they believe a judge would refuse, and that is the top and tail of it. They should not be allowed to do that.

Chair: Thank you very much. We are going to vote now. Thank you for giving evidence. We might write to you for further information but we are most grateful. I am adjourning the Committee for 15 minutes and then we will return.

Sitting suspended for a Division in the House.

On resuming-

Examination of Witnesses

Witnesses: **Maxine De Brunner**, National Lead for Lawful Intercept, **Richard Berry**, National Policing Lead for Communications Data, and **Chief Constable Mick Creedon**, Derbyshire Police, gave evidence.

Q104 Chair: The proceedings have now recommenced. My apologies to our witnesses for having interrupted the proceedings but I am afraid items in the House take priority. Thank you very much for coming at short notice. The Committee is doing a very short look at RIPA and we thought that the three of you might be helpful. We did not actually want the three of you but we felt in the interests of getting everyone topped and tailed we should have the three of you. What the Committee did is it wrote to the chief constables to ask them for information which we felt was relevant to our inquiry. We received a letter back from Keith Bristow and Hugh Orde in which they said that the two key people to speak to were yourself, Mr Berry, and Maxine De Brunner, and then I had a call from Cressida Dick who said, “Do you really want Maxine De Brunner because she is not allowed to say anything?” and I said, “Well, this sounds even more interesting”. There is nothing like guaranteeing a slot at Home Affairs to be told that if you have a witness they cannot tell you anything. “Shouldn’t you also have Mick Creedon?” So with these kinds of recommendations the Committee could not say no.

We are not looking at particular cases here today. We are trying to understand either what is good about RIPA or what we can improve about it, because the Committee has a position that we think this legislation should be reviewed. But we are concerned about public reports that are in the public domain about police forces using or misusing RIPA powers. So that is really what we want to talk about. It is more about process and numbers rather than the intimate details of any particular case.

Perhaps, since you were recommended so highly, Maxine De Brunner, I should start with you. What exactly do you do in relation to RIPA?

Maxine De Brunner: Good afternoon, I am the National Lead for Lawful Interception, which is covered by RIPA 1 of the codes. So that is the interception of communication, being slightly separate from Richard in terms of comms data. I report in my portfolio to Mick Creedon who runs the prime business area. That is where you get the join up between the three of us. The type of matters we deal with are intrinsically linked, which is why the three of us together would probably give you the picture that you are after.

Q105 Chair: Indeed. So in respect of the practicalities—obviously we do not want you to break any secrets because we know section 19 is often thrown in front of us to say, “No, we can’t talk about this, that and other”—a superintendent would authorise the use of RIPA powers, is that right? At that kind of level, or is it lower or higher than that?

Maxine De Brunner: In terms of RIPA generally, yes. But in terms of RIPA 1, which is what I lead on—

Chair: Do the bit that you know about, RIPA 1.

Maxine De Brunner: Okay, the piece that I know about, my role—and it is slightly complicated inasmuch as the Home Office lead on the strategy for lawful interception, not policing, because there are so many agencies involved. The law enforcement is one voice in the RIPA 1 piece, in the lawful interception piece. That is my role, I hold that voice on behalf policing in England and Wales, Police Scotland hold their own independent voice, as do the police service for Northern Ireland. We all sit around the table with other agencies, which is why it is a slightly more complicated picture.

Q106 Chair: I understand the strategy, but tell me about the practicalities? Tell me about somebody who wants to go under part 1 and either get a warrant or not get a warrant. How do they do it and where do you fit in? Where is the oversight from senior officers?

Maxine De Brunner: In terms of where I fit in, very remotely in terms of individual cases. So it is my job to make sure that, as far as we can, there is some consistency across forces in how we manage warranting. So at the moment in England and Wales, the intercepting agency for England and Wales is dealt with by the National Crime Agency, hence Keith Bristow and Sir Hugh Orde replied to the letter that you originally wrote. So they intercept on behalf of other forces. Albeit that there are other agencies that also do carry out interception.

So an application would come in and there are really robust safeguards, it has to be for serious crime, it has to be for the economic wellbeing of the country or it has to be on grounds of national security—

Q107 Chair: That comes to you? You see it?

Maxine De Brunner: It does not come to me.

Q108 Chair: It does not come to you?

Maxine De Brunner: It does not come to me.

Q109 Chair: Who does it go to?

Maxine De Brunner: It will go to the force in the first instance that is asking for the interception. So, hypothetically, in London if they wanted to intercept something on a particular case, such as a kidnap, crime in action, that would go into the Met for that particular application if that was going on.

Q110 Chair: They would deal with that locally without you being involved?

Maxine De Brunner: I would not be involved in that. They would manage that. They would draw up the paperwork in terms of making sure that was proportionate and necessary, that it met the serious crime criteria and then that application would be forwarded, once it is properly processed, to the National Crime Agency who also have their own independent scrutiny of that application. Ultimately, of course, any application for RIPA 1 for interception of communications is authorised by the Home Secretary.

Q111 Chair: Who would it go to at the NCA? Mr Bristow himself or someone below him?

Maxine De Brunner: It would probably go to someone below him.

Q112 Chair: Right, and from there it would then go to the Home Secretary because she signs these off?

Maxine De Brunner: She signs these off, that is right.

Q113 Chair: Thank you, that is very clear. Much clearer than the letters, I have to tell you, which left me in some confusion. Mr Creedon, where do you fit in?

Chief Constable Creedon: If I could just take two minutes, the way we structure in policing, because it is so complicated, within the crime and business area and the portfolio I lead on serious and organised crime there are three relevant police leads: Maxine; Richard, who leads in terms of comms data, which is a complicated area; and we have a lead for RIPA, which that is an assistant chief constable. These people lead in terms of policy, development and standards. They work with the College of Policing and they speak on behalf of the service. They do not lead in any way in terms of the operational deployment, which is an individual issue for each force. So we are policy development, practice development and speaking on behalf of policing. I lead on serious and organised crime and the three individual groups of RIPA, LI and comms data sit within my portfolio. I speak, on a broader front, on behalf of all of these.

Q114 Chair: How would you know if police forces are misusing RIPA?

Chief Constable Creedon: What we do around RIPA, since it has been in—which is nearly 15 years now—there has been a huge amount of development. There are detailed codes, as you are well aware. We have a lead for it, each force has a RIPA lead, the working group under RIPA will look at how we are improving and so on, and fundamentally we look at things like the OSC inspection reports, we have a huge amount of professional development around it, we set standards, we develop forms. Undercover deployments are through RIPA. For example, all those forms have been reviewed and renewed and are constantly changing to meet the increased scrutiny. So we would not know about an individual failing on a force by force basis. That would be reported either by the force who realises the failing to the OSC or by the OSC through their inspection. That report is made available through the OSC to each Chief Constable and increasingly to their Police and Crime Commissioners.

Q115 Chair: If the commissioner only looks at 10% of the cases you are totally reliant on a local police force to say, “Something has gone wrong and therefore we need to put this right”?

Chief Constable Creedon: In the sense of the LI or much broader?

Chair: Either.

Chief Constable Creedon: Yes. When the OSC come and do their inspection they look intrusively at a whole range of activity but clearly they cannot possibly audit the entirety. There are some cases within RIPA that require the OSC’s pre-authorisation, but they are the more intrusive tactics. You were asking about superintendents, that tends to be for the more volume directed

surveillance. Beyond that it will ramp up and there's a number of areas where only the chief constable can authorise.

Q116 Chair: Can it be lower than chief superintendent?

Chief Constable Creedon: Yes, it can for an urgent reason. Life at risk, for example, it can be lower.

Q117 Chair: Down to what rank?

Chief Constable Creedon: Inspector. But as soon as possible that will be passed to the superintendent and each force has its own covert authorities' bureau that keep all the documentation and they will be involved in that as soon as possible.

Q118 Chair: Mr Berry, where do you fit in? I was confused, I was clearer and now I am a little more confused. It seems very complicated this whole structure.

Richard Berry: Chair, thank you. I agree with you, first of all, in terms of the complexity of this structure. My role is National Policing Lead for Communications Data and in that role I deal with training, I deal with capability building, I liaise with industry because they clearly have a significant role to play.

In terms of dealing with communications data, that is a separate chapter of RIPA. It has a separate code of practice that details the whole process, the standards, the oversight, the recording and reporting of errors purely for communications data that is separate to lawful interception. We both therefore report to IOCCO as the oversight board. In the wider RIPA regime that reports to the office of surveillance commissioner. So there are two separate oversights over these two tranches of RIPA itself. In terms of communications and interception, that reports to IOCCO.

Q119 Chair: I had a parliamentary question that has just been answered, I do not know if you have seen it. Since the enactment of RIPA in 2002 the number of communications data items processed just by the Home Office has gone up from 53 in 2002 to 6,056 in 2013. I was quite alarmed by that figure.

Richard Berry: In terms of communications data, yes.

Chair: That is just the Home Office.

Richard Berry: We—

Q120 Chair: Do you have any figures for me today about—

Richard Berry: Yes, they are all printed through annual reports of IOCCO. It sits around about 500,000 and it fluctuates on an annual basis. Last year was 514,000 communications data applications. There is some complexity beyond that process that I will go into in a second. It is generally sitting—I think for the last three years—at around 500,000.

Q121 Chair: How can you make it simpler for the public and Parliament? Where are layers of bureaucracy that currently exist that will allow this process to be simpler? You first, Mr Berry.

Richard Berry: Yes, certainly. From my perspective in terms of communication data, it is certainly mentioned in the IOCCO report, because of the complexity of legislation, because of the complexity of the processes and because of the rapidly changing environment in relation to communications data, new technology and everything that David Anderson is looking at in his RIPA review, there is a need to have a very clear public narrative. It is certainly something I am working on with ACPO's communications department to start working out how we simplify that narrative so the public and key stakeholders really understand what is a very complex area.

Chief Constable Crendon: There are three simple key points I would make around that. Technology, Richard touched on. We need to make it clear this is absolutely the lifeblood of a whole range of investigations and also protecting the public. I hear a lot of talk about RIPA being around terrorism. Terrorism is only one part of it. If you look at the authority levels, it is as much for public protection, for CSE inquiries, for homicide investigations, terrorism and we need to understand that.

The most important point is we must not confuse comms data, which you obtain through RIPA, with detail and content that you obtain through a post-production order. Having heard the last speaker, I think there is a real confusion. That issue about accessing the content under PACE is quite different to accessing the data through RIPA. I understand why people would get very jumpy when we start looking at content because it is much more intrusive but data is absolutely essential. Were any law enforcement agents to be here they would be telling you exactly the same. The figures are something like 100% of terrorist investigations, 95% of serious crime investigations, virtually every homicide investigation is reliant upon comms data for a whole range of reasons. I do not think we have managed to describe that to the public.

Q122 Chair: Maxine De Brunner, any improvements? How do we make it less complicated?

Maxine De Brunner: In terms of RIPA 1, I am not sure I would want to make it less complicated because the piece that I am overseeing is at the most serious end and the most intrusive. I am very satisfied that that is as robust and as complex, with as much oversight, as there can possibly be because it sits at the intrusive end of covert activity.

Chair: Thank you.

Q123 Dr Huppert: There is a lot that comes out of what you have said. If I could start off on the issue about interception, Ms De Brunner. We are always told these warrants are looked at very carefully, individually, there is a great deal of care. You would say that to this Committee, as well?

Maxine De Brunner: Yes.

Q124 Dr Huppert: Apart from the fact there have been 57 errors, which clearly raises questions, I am struck by the fact that in the letter from Keith Bristow and Hugh Orde when we asked questions that seemed fairly basic—like how many investigations were there with interceptions where somebody was ever arrested—the answer was, “This information is not recorded”. When we asked how many times were they charged with an offence? Don't know. Convicted of an offence? Don't know. It seems very odd that you have this incredibly careful process that you look at everything

very carefully and then you do not look at what happens afterwards. Do you agree that is rather strange?

Maxine De Brunner: No, inasmuch as the use of interception is one part of a very long process within an investigation. The outcomes for the end of the investigation, they are collated and they are published, but in terms of individual activity they are not.

Q125 Dr Huppert: Sorry, but what we were told was that there isn't any information on how many investigations have resulted in an arrest that use interception. Are you saying that is not right, what we were told in the letter by Keith Bristow?

Maxine De Brunner: No, that is right, we do not keep those particular figures but we do, in the wider sense in terms of the operations, record outcomes.

Q126 Dr Huppert: How do you assess whether these warrants were, in fact, useful, whether you are applying for ones that you do not need, if you have no idea what the outcomes are? It seems like a huge gaping hole in any policy making process.

Maxine De Brunner: In terms of outcomes, we know that the use of lawful interception saves lives. For us in policing, that is one of its primary purposes. We know that we have to do that really quickly.

Q127 Dr Huppert: But you do not know how many arrests it leads to? We are told you do not know how many investigations have led to an arrest.

Maxine De Brunner: Not from interception on its own.

Q128 Dr Huppert: It seems to me that are data that should be collected and you would find your case rather easier. There is lots more I could say on this but I suspect we have limited time. If the Chair allows, I will come back.

Mr Berry, earlier you talked about communications data. Mr Bristow told us when he came to see us that the largest problem they have had with risk to life was to do with IP address matching. There is a disagreement about whether it is 90% of the cases they had a problem or 100%, but it is in that range. I do not want to focus on that bit. Would you agree the fact it is very hard to do IP address matching is a big problem for investigations?

Richard Berry: IP resolution is a challenge and there is a lot going on within technology around the sheer use of the internet, the sheer availability with the internet protocol version 4, and the way communication is dealt with with a limited number of IP addresses.

Q129 Dr Huppert: Indeed, and IPV6 may fix in the problem.

Richard Berry: It may do.

Dr Huppert: But in the meantime there is a problem. How many discussions have you had with the Home Office about implementing the statement in the Queen's speech from two years ago that there would be a procedure to deal with this problem?

Richard Berry: That is a matter that is being dealt with within the communications capability development programme. The question in terms of that particular matter would have to be answered by written submission, if I may, to give you some more detail.

Q130 Dr Huppert: A letter would be very helpful but have you had direct conversations with the Home Office about IP matching?

Richard Berry: It is a constant subject of discussion around IP resolution and I have certainly had personal operational experience of that particular issue becoming problematic, yes.

Q131 Dr Huppert: But in terms of discussions with the Home Office about fixing it. I am very alarmed the Home Secretary does not seem to have made any progress on something that was agreed two years ago, which everybody agrees is critical. Perhaps you can write to us but you have specifically asked for this from the Home Office? Have they made any specific proposals to you?

Richard Berry: I would have to bring that into the written submission, if I may.

Q132 Dr Huppert: Fine. Just to complete the trio, Mr Creedon—I will not dwell on previous discussions about speeding and whether comms data is applicable to that—can I pick you up on this idea there is a clear distinction between communications data and content? You said, and I do not remember the exact words, that content is intrusive, generally yes, and communications data is not. I do not think anybody is saying there should be no communications data collected. I have never heard anybody make that case. Do you accept the communications data can be incredibly intrusive as, for example, if it reveals that somebody is phoning an abortion counselling line or a depression line, or whatever it might be?

Chief Constable Creedon: Absolutely. I did not mean to say not intrusive. I think there is a difference there between the content and the data, but the data now and data through a whole host of medium can tell a huge amount about what a person is doing. A huge amount. Increasingly so. Content is even more so, but I do not deny that data collection is intrusive.

Q133 Dr Huppert: So, for example, it could be the only thing that was needed to reveal who a journalist's source was?

Chief Constable Creedon: It is an interesting discussion that. I have been acutely aware of this recently and I heard what was said earlier. I have to say, we are not interested in journalistic sources. I struggle to understand quite what the debate is. We would be interested, for example, in a police officer who was passing information to a range of individuals. In looking at that police officer and their call data, it may well be one of those is a journalist or we may even think at the start of the inquiry, "We believe officer A is giving information to the media". But the issue about wanting to know who a journalistic source is, with one or two extreme exceptions, I really cannot understand why we would want to do that.

Q134 Dr Huppert: Would it be acceptable to use these powers as part of a leak inquiry?

Chief Constable Creedon: The powers to collect call data? Absolutely. Absolutely. I would imagine the public would expect us to do that. If we have corrupt officers who are passing

information to the media, either for cash or other reasons, they would expect us to use it. The issue is not about the journalistic issue, this is about the corrupt individual who is passing information. I accept the corrupt individual could be the well-intentioned whistleblower, the honest whistleblower so we need to be careful of that, but we are not interested in journalistic sources.

Q135 Dr Huppert: You give an example of corruption of a police officer, would it be legitimate to use it in other areas where there was information being passed out to a journalist?

Chief Constable Creedon: I suppose if there was another organisation where there was a corrupt individual reported to us and we were investigating on behalf—

Q136 Dr Huppert: It would require a belief that there was criminality?

Chief Constable Creedon: Absolutely. The test for RIPA is about that level and it would be very unusual to use anything other than that test. The RIPA is much wider, as I said, than just terrorism. If you look at all the categories, it would need to fit one of them very firmly.

Can I say one last thing? If we believe we are accessing data that could involve a journalist the test would move it from a superintendent upwards. It would go to a higher level because routinely we—

Q137 Chair: That is if you know, but if you do not know it is a journalist—

Chief Constable Creedon: If we know.

Maxine De Brunner: Yes.

Chair: —you cannot do that, can you?

Chief Constable Creedon: We do not at the start but if we did know, if we did suspect officer A and journalist A and we believed it was what it was, we should be going to a higher level.

Q138 Mr Winnick: So what you are saying, Chief Constable, if I understand you correctly, is that the concern expressed today by the General Secretary of the NUJ and various newspapers that the police are intruding on their sources is without any foundation at all?

Chief Constable Creedon: In my experience, which is relatively extensive, and being involved in a lot of the investigations and reviews into external forces, I have never known it. I have a lot of close friends who are journalists and I have this discussion with them. I cannot imagine why we are interested in a journalistic source unless that source is corrupt in the way that I described.

Q139 Mr Winnick: Therefore the concern expressed today, as I have said, you think it is, to put it bluntly, paranoia?

Chief Constable Creedon: No, I absolutely understand why journalists would want to protect sources. I agree with the sentiment and ethos behind it, but I do not know of any cases where we have sought to find a journalist's source because we do not necessarily like what the journalist is saying. There are always times when there will be collateral intrusion through RIPA activity.

Looking at one part of covert activity may give information that could be what we call collateral, but we would not routinely look to find out who a journalist was getting material from.

Q140 Mr Winnick: The story *The Daily Mail* had on 10 October about their sister paper, you know all about it because it came very much into the frame, would you say it was justified what the police did?

Chief Constable Creedon: It would be wrong for me to comment on another force's investigation, of which I have basically read about in media. That is all I have seen so I would not know the detail, but in that case my assumption is the investigation was about perverting the course of justice and corruption by two individuals who both ultimately to prison. It was not about the journalistic aspect but the journalistic aspect came in as a consequence of it. But, as I say, I am answering hypothetically because I do not know the ins and outs of that case. You know more than I do.

Q141 Chair: I do not think Mr Winnick knows more than you do, I think he read it in the same newspaper.

Chief Constable Creedon: He probably read it more closely than I did.

Q142 Mr Winnick: I may or may not, but one thing is clear is that it has caused a great deal of concern and anxiety and has not been brushed off, if I may say so, Chief Constable, in the manner in which you have done so today.

If we take, for example, the North Kent police, they have said that consideration should be given to how material held by the media might be relevant to a criminal investigation and share it with the police and courts. The view of the NUJ, as you may have heard if you were listening, is that if that is the case, if the police feel there is some aspect where criminality is involved then the police should go through the judicial process, not simply act accordingly on their own.

Chief Constable Creedon: I agree. No, I think the distinction is RIPA is about the covert activity to try and gain intelligence from a range of sources. For me, if that was the case and we believed the newspaper was holding information, it should be a PACE production order subject to the oversight that you heard talked about. I agree completely. If I as an investigator believe that material held by a newspaper, which I think is material to my investigation, absolutely PACE production order. RIPA is not the machinery by which to present evidence to courts. PACE is the right machine for that and the PACE production order allows for that judicial oversight and with safeguards.

Q143 Mr Winnick: Do you accept there is bound to be anxiety—it may not be justified and the Chief Constable does not believe it is—that the police are intruding into matters where the right of journalists to try and obtain stories, put them in the public frame and the rest of it, are considered essential by the journalist and hence the anxiety that has been expressed today by the head of the NUJ?

Richard Berry: If I may answer some further detail here. There is a huge difference between what is described as content, journalistic material, and a superintendent or designated person according to the codes of practice here authorising access to communications data.

Communications data is essentially three things. It is traffic data, it is service use data and it is subscriber information. It is not journalistic material per se.

The law is very complex in this area, it needs perhaps further work on interpretation, not that I can offer today, but it seems to be misreported in some respects in terms of making something reported very simple, very complex.

Q144 Chair: Mr Creedon, Mr Winnick obviously puts his question better than I could, but I am concerned about the way you reacted to what he said. He only has the same source as you do but you are the top man. If there was an article in *The Mail on Sunday* about the misuse of RIPA and the information being passed on to a third party—by the way I think it was Essex Police not Kent Police, I made the mistake in writing to Kent and they were very quick to say it was Essex—surely you, as the man right at the top of this very complicated tree, would want to know exactly what went on. The passing of information to third parties goes beyond looking for criminality, does it not?

Chief Constable Creedon: I was not passing it off lightly and I was referring the detail of the original prosecution case and following the case through the court. That is what I was referring to.

The issue around the data, as I understand it—Kent and Essex have a joint unit that did the investigation, which maybe confused things—is a concern because of the various stuff that has been in the media. But I come back to my point a PACE production order—

Q145 Chair: Yes, I understand it is a concern so what have you done about it? When you found out that information has come out, lawfully in your view, from the police using RIPA and it has been passed to a third party—you have seen the newspaper article, it is a very bizarre article. The editor of the newspaper only discovered that his telephone number was included in the investigation when he was sitting next to a solicitor who was having coffee in the same cafe. You could not really make it up, could you? Even I, who do not necessarily read *The Mail on Sunday* every Sunday, was taken by this story. What have you done about it? About the passing on of this information to a third party to make sure it is a rare occurrence?

Chief Constable Creedon: I come back to the starting point that I tried to describe. I have no locus whatsoever in terms of how a force carries out its investigation, very well or very bad. That was an investigation that would be subject to any scrutiny and also subject to full CPI disclosure, including that detail. That was a matter that went through the CPS, through counsel to court and was scrutinised. The role we play through the way we are structured, and it is complicated, with the business area is to look at improvement, training and so on, as you heard.

The RIPA lead for this matter is an assistant chief constable who is not here in front of you today, he is not trying to avoid the issue I promise you but it is a complicated world the crime world, and that is something that will be part of their plan to improve. I am not sure the failing is necessarily the failing as it is being played out in the media.

Q146 Chair: We will never know because no one has followed it up. This is the worry for this Committee, I write to one person, I get three obviously very senior people. I then ask the man who I have been told to have here by Cressida Dick—I do not know what you have done to upset her but she suggested you—

Chief Constable Creedon: I was going to say that.

Chair: —and you are telling me to go to the Assistant Chief Constable of Nottingham.

Chief Constable Creedon: No, no.

Chair: We then have the Interception Commissioner who says he only looks at 10% of the cases. No wonder people worry about the system.

Chief Constable Creedon: I do not know of any auditor that audits 100% as a matter of interest. All it is meant to be is looking at risk, isn't it, rather than an entire overview of everything? That is for them not me.

I think the issue around, again I am very happy to write and get some more details, me carrying out some operational review or investigation—

Q147 Chair: But who does that if you do not?

Chief Constable Creedon: The responsibility is with the chief constable and the oversight through the Interception Commissioners and the OSC.

Q148 Chair: Fine, so there are three other bodies involved. Do not worry, the Committee will write to the Chief Constable of Essex and get to the bottom of this. Mr Berry, you were going to say something before I close?

Richard Berry: If it would help, I have a copy of an inspection report here. There is also a senior responsible officer in each organisation responsible for the reporting in relation to communications data—making that point—and responsible for the oversight and the integrity of the applications.

Q149 Chair: Thank you. When I wrote to the chief constables they wrote back and they said they do not collect information on professions and indeed they do not store information. Then I received the letter back from Sir Hugh Orde and Mr Bristow. We have just heard in evidence today that the Interception Commissioner has written to the same chief constables that the Committee wrote to and he does have that information. So there is this information, is there?

Richard Berry: The information—

Chair: You have given it to him because he has powers.

Richard Berry: He has statutory powers.

Q150 Chair: So the information does exist?

Richard Berry: It takes a lot of work to work through and we are working with the interception commissioner's office to work that through. The data is not readily available. There is not a field of data to say, "This person is a journalist" or, "This is a legal representative" if we were looking at legal privilege or indeed a Member of Parliament. We do not categorise that data during the application process.

Q151 Chair: I understand. Mr Bristow's letter, I hope you have seen a copy—

Richard Berry: Indeed.

Chair: —in response to six of my questions he says, “This information is not routinely recorded”, “This information is not routinely recorded”, “We do not have this information, we do not record it”. Sorry, two of those questions. But you are now saying you do have that information but it just takes a long time to get it?

Richard Berry: We have to research. It takes a lot of effort and we are going to have to look at all of the applications to try and discern whether or not we consider that person may or may not be a journalist based upon the previous discussion of what is a journalist. Is it a card carrying member of the NUJ, is it someone who is a citizen journalist, and so on? It is all about getting that definition or clarity in relation to the data.

Q152 Chair: Of course. Has everyone now replied to the Commissioner?

Chief Constable Crendon: Mr Vaz, I would assume so. If I could just try and help, the RIPA forms are very complicated, I do not know if you have seen them.

Chair: No.

Chief Constable Crendon: They do not involve occupation. It is not one of the fields that is filled out.

Q153 Chair: But do you have an occupation field?

Chief Constable Crendon: No, there is not. It does not involve occupation, probably for good reason. There will be those, though, when we know at the start where they are subject to sensitive information collection, there will be a field where we would but that would not just be journalists. But to look backwards at occupation and look backwards at the reason would be pretty difficult. I think that was maybe why some forces did not feel able to comply. It is not routinely collected in the RIPA forms. If you know at the start of the investigation it was journalistic or legally privileged, you would be able to have that. That is a field that all forces would have very quickly.

Q154 Chair: One final question to each of you. Apart from Maxine De Brunner who says she is happy with section 19 and the way in which it has been dealt with, in other areas of RIPA do you all think that it does need to be refurbished and improved? Mr Berry?

Richard Berry: From a communications data perspective, we are working closely with Mr Anderson and his RIPA review.

Q155 Chair: No, we know all that. What do you think? You are here as an expert, are you not? Do you think it is too complicated and it needs to be looked at again?

Richard Berry: I think by its very nature it is complicated. Perhaps there are issues that will come out in due course, particularly around the ever increasing complexity of communications data that could be simplified and we would certainly work with Mr Anderson on that. In terms of does it need a complete overhaul? I think it is a robust piece of legislation and certainly from a communications data perspective, I can furnish the Committee with statistics, this is every day

policing, this is not just counterterrorism, not just serious and organised crime, it is around protecting vulnerable people.

Q156 Chair: Mr Creedon, a question to you. I spoke to Lord Falconer who brought in this Act under the last Government and he said it has been used for purposes that he and the Government of the day never intended.

Chief Constable Creedon: I certainly agree. I remember being with Shami Chakrabarti talking about this and she was very clear the police are not misusing it, was the position she took at this conference. Maybe local authorities have been misusing it and cameras in bins and surveillance around things like school catchment areas, it is probably not appropriate. It was never intended for that, but, I think, in terms of serious crimes it was.

I agree with Richard, I think it is robust. I am old enough to remember covert activity before RIPA when there was no statutory framework so there is something very powerful about having this. I will give you an example, if I may. If I authorise a fairly non-intrusive covert device that tracks where a car moves, for example, in Derbyshire and then that car moved to Staffordshire, to Birmingham and then to North Wales, that authority needs repeating four times. That whole sheet of paper, that whole consideration of proportionality and necessity needs repeating. That is the nonsense in today's world. The most we can do is six forces but we do not know whether the criminals were going. There are some simple non-bureaucratic things that could change with RIPA to put policing on the same status as the NCA and others, where the authority runs across England and Wales. There are issues around data comms, it has become hugely more complicated, and there are issue around some of the more covert activity that sits at my level bizarrely is less intrusive than some of the activity that is authorised by lower down, if that makes sense. Undercover is one of them.

Q157 Chair: Yes, and we will have you in on that. Again, finally, the IMSI catchers, do you have many in Derbyshire?

Chief Constable Creedon: It would not be appropriate to talk about that. That is a tactic that has been reported in the media, it is a tactic we would not normally talk about because it would not be appropriate to.

Q158 Chair: You must know, do you have them or not?

Chief Constable Creedon: I know exactly what they are but I have never accessed them.

Q159 Chair: Can you perhaps tell the Committee?

Chief Constable Creedon: I do not think it would be appropriate to talk about such a covert activity in a public arena.

Q160 Chair: Right. It has been in *The Times*, you see. We may not want to talk about it, but it says that. "IMSI catchers Hoover up the identity call and message data of mobile phones. It is very powerful" which is presumably on the market. You and I may not want to talk about it but is

probably on the internet where you can buy one, “can intercept and listen to phone calls and collect and read text messages and emails and block phone signals in a specific area.”

Chief Constable Creedon: To reassure you, I did read all the article and I nearly thought about ringing the journalist.

Q161 Chair: So they do not exist, these machines?

Chief Constable Creedon: At the end you will see both the Metropolitan Police and the National Crime Agency neither confirm nor deny the existence or the use of this tactic.

Chair: Of these devices. Rather like the Daleks, we do not know whether they are there. Yes, Dr Huppert, a final question.

Q162 Dr Huppert: Just to follow up on this because it is quite an important question about what is authorised and what is not authorised. I understand the reluctance to talk about anything that collects whole ranges of data. Who would supervise this? Who would check whether this was being used proportionately, appropriately? The suggestions are that IMSI catcher could be used ultimately to send fake text messages. Who would authorise any of that? Who would scrutinise it? Who would make sure it was being done and who would make sure that Parliament was able to judge whether it was something we would like to take action on or not?

Chief Constable Creedon: The most intrusive covert activity is authorised by the chief constable and in extreme cases by their deputy—normally the only time that happens is when you are out of the country. They are subject to either prior approval or notification to the Interception Commissioners. The Interception Commissioners collect all that data and that is reported on a regular basis. The Interception Commissioners report to the force individually but they also report on national report to the OSC.

Q163 Dr Huppert: So that commissioner will have complete oversight of how IMSI catchers are being used and for what purposes?

Chief Constable Creedon: Absolutely. Every year they go to every force and they look intrusively on a three or four day inspection at a whole range of covert activity from the most intrusive down to surveillance, undercover and so on.

Q164 Chair: Mr Creedon, we will have you back in the future to talk about undercover policing as we promised to do. Maxine De Brunner, thank you very much for coming here. I hope you will reassure the Commissioner that you gave no secrets to this Committee; they are all safely with you. Mr Berry, thank you for calling in to see us today. We will write to you separately because I notice you have a particular interest in mental health and policing. Is that right?

Richard Berry: Yes.

Chair: We might drop you a line because we are doing an inquiry into this. I know it is not what you are doing at the moment and you did it many years ago but your thoughts on it would be of interest to this Committee. Perhaps you can tell us your M.Phil. thesis that I think you wrote on it.

Richard Berry: That is well researched, sir, if I may say so.

Chair: If you could write to us with that information, we would be very grateful.

Richard Berry: I did owe you some information on the bottom of this letter.

Chair: You did and you brought it here.

Richard Berry: I have brought an answer for you. The data of recordable errors in relation to communications data are available. Every error is inspected in a force report. I have spoken to the Interception Commissioner's office and we could facilitate between us the delivery of that data.

Q165 Chair: Can you tell us now?

Richard Berry: I do not have it to hand, sorry.

Chair: I see. We look forward to your facilitations and we send you our felicitations for being here today. Thank you very much for coming.

Richard Berry: Thank you.

Maxine De Brunner: Thank you.

Chair: That concludes the Committee's inquiry.

