INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT

PRIVACY AND SECURITY INQUIRY

PUBLIC EVIDENCE SESSION 8

UNCORRECTED TRANSCRIPT OF EVIDENCE

Evidence given by:

Sir David Omand
King's College, London,

Thursday 23 October 2014
(11:15 – 12:00)

Q1 Chair: I welcome Sir David Omand to this public evidence session of the privacy and security inquiry of the Intelligence and Security Committee. Sir David, we are delighted to have you with us today. We were grateful for your written submission and we look forward to our 45 minutes of oral evidence.

I understand that you would like to make some opening comments. I am sure that the Committee would be pleased to hear them.

Sir David Omand: Thank you, Chairman, and with your permission.

I submitted written evidence to the Committee because I am becoming increasingly concerned that there is a quite unnecessary moral panic over privacy that has been aroused by the publicity surrounding the material—the documents—that Edward Snowden stole from GCHQ. I think this is because there is a quite fundamental misunderstanding of the context, and the commentators have really not distinguished activity on the internet at three different levels.

At the top level, we have our everyday activity—socialising, sharing, entertaining, trading, banking—and we are under constant attack at that level by cybercriminals using malware, or simply using the internet to conduct theft and fraud at scale. Those who mean us harm—the dictators, the insurgents, the terrorists, the narco-criminals, the proliferators, the paedophiles and all the rest—are using exactly the same mobile devices, communications and apps as we are in our everyday internet activity.

Beneath that everyday level, there is a law enforcement level that is desperately trying to police the worst abuses on the internet and failing—and failing increasingly. This battle is being lost because cybercrime is racing ahead and the dark web is expanding. Briefly, there are the sorts of problems of which the Committee will be well aware: there are not enough experienced cyber-detectives and the tools for cybercrime can be bought, so you do not have to be a hacker yourself to

exploit it for criminality. Law enforcement cannot access the communications data and the communications that, in the old days, it would have been able to access rather easily from the telecommunications companies. The companies simply do not have the business need to retain the data, and the modern internet service providers are mostly based outside the United Kingdom anyway and there are all the difficulties of obtaining warranted data from them. Most of the serious criminals that we are talking about, and others, are in jurisdictions that do not respect mutual legal assistance, warrants or extradition requests.

Finally, law enforcement faces increasing difficulty in accessing heavily encrypted material that may be found on their suspects' mobile phones or computers. As you will have read, post-Snowden, the companies are now making their devices technically inaccessible even to themselves. So warrants are rendered moot. The net result of that is that this second layer—the law enforcement layer—has been forced, increasingly, to look to the third layer, which is the national intelligence layer, and that exists primarily, as the Committee knows better than anyone, for the purposes of safeguarding national security, supporting our armed forces and supporting our diplomacy.

One should remember that Parliament did actually legislate in 1989, and again in 1994, to authorise the intelligence agencies to support law enforcement in the detection and prevention of serious crime. Remarkably, well in advance of our European partners, Parliament decided more than 20 years ago to legislate for the intelligence agencies and impose on them exactly the same legal regime for interception as for the law enforcement layer, so the intelligence layer is also subject to necessity, proportionality, oversight, regulation and so on.

You can see where the misconception now arises, because Snowden lifts the lid on the use—as a systems analyst, he has access—of the national intelligence agencies' powerful tools at that top level, and sees it as mass surveillance. Of course, it is the opposite; it is the highly discriminating, selective use of those tools in order to find the communications data and communications of their suspects to protect us from threats of terrorism and criminality.

I say that really as further explanation of what I put in my written evidence, which was, frankly, that there is a category error: confusing bulk access to the internet, which I am very pleased that, as a nation, we do quite a lot of, with mass surveillance which, as you know, Sir Anthony May, the Interception Commissioner, examined and concluded does not happen, and were that to happen, it would be comprehensively unlawful.

Q2 Chair: Thank you very much indeed. Those extremely helpful introductory comments go to the very heart of the issues that we are addressing today. May we now go into the more specific questions that we would like to share with you, David?

First, a general question—I suspect I know your answer. We call our inquiry "Privacy and Security", implying there is a sort of choice between the two. What is your own assessment? The European convention on human rights talks about privacy being a qualified right. In terms of the intelligence aspect, would you share with us your thoughts as to how that balance can best be achieved?

Sir David Omand: I think it is a huge mistake to talk about trading privacy, or indeed any other human right, for security, because what we are trying to achieve—or should be trying to achieve—is a balance within the basket of human rights. Privacy is not an absolute right, as you say, Chairman. We have to seek the right balance, because security is also a right. I have a right to life and not to be blown up or shot by some crazed terrorist. So what is that right balance? That is what society has to establish.

I do not like the concept of trading security and privacy as well, because when you look round the world, when you see countries that do not have sufficient security, these are the countries that are completely unable to protect human rights. So the two go together.

Q3 Lord Butler: Do you think there is a paradox here? On the one hand, for the prevention of crime, people need more protection of their communications from people who mean ill but, on the other hand, it seems to me that there has been a seismic shift in attitudes to privacy, as people are willing to share very much more detail about their life than they ever have before, thus making themselves vulnerable. How do you reconcile these two movements in society?

Sir David Omand: Well, in a sense, I come back to my layers. I would say, at that first layer of everyday activity, that we must have a very high assurance of protection for our communications, and that means that I am all in favour of encryption. I am all in favour of ways of protecting our communications for everyday purposes. Indeed, if we fail in that, confidence in the internet itself will be eroded, and its use for commercial purposes. We are, I think, wholly dependent now on the development of applications on the internet for our future economic growth. All our companies are completely dependent on this. So if confidence falters, we are in serious trouble so, at that first level, we do need that. But then you come to whether that is absolute. Have we made that an absolute right so that that encryption cannot be overcome by any legal warrant? My answer is no; you have to enable the law enforcement layer.

Lord Neuberger, the President of the Supreme Court, made rather an interesting speech in Hong Kong quite recently in which he said that, for this kind of debate, it is quite useful to think not about privacy rights, but of privacy rights being a subset of freedom of expression, which is a much more fundamental right, and that if I feel I can't express myself because I fear others will get to know, my freedom of expression has been fundamentally eroded.

As Judge Brandeis said all those years ago, freedom of expression doesn't give you the freedom to shout "Fire!" in a crowded theatre. Privacy and the freedom to express yourself privately do not give you the freedom to express words, thoughts and deeds that are intended to harm others.

Q4 Lord Butler: But some people might argue that is a Big Brother argument—that you are saying that the only body that should be able to infringe people's privacy is the state, for reasons the state thinks are good. But not all states may always operate in a beneficial way.

Sir David Omand: I have always been guided on this by the various judgments of the European Court of Human Rights, which has taken a very sensible view on this. It has said that states do have that right to protect their citizens, but there is then a series of conditions: it must be laid down in law—there must be no secret law in black letter law—and there must be independent oversight, regulation and all the rest of it. The United Kingdom complies exactly with those conditions, as laid down by the European Court. The alternative is to go back to the view that was originally espoused by the internet pioneers, which is that the internet is a new world—a new dawn—and an unregulated space. That is the sort of Ayn Rand view of the internet. They did not see the way in which the internet would be perverted by criminals, terrorists, crooks and paedophiles.

Chair: Thank you. Let's now move briefly to the question of targeted intrusion. I say "briefly" because there has not been too much controversy, and most of our witnesses have accepted that it is justified, but there are a couple of points we would like to raise with you.

Q5 Mark Field: You mentioned this whole idea of there being something of a wild west show and this sort of wild libertarian view at the start of the internet. That is in stark contrast to what one might regard as the more traditional means of tapping telephones and steaming open letters. Would you take the view that the monitoring and surveillance of an individual's internet communications are a more intrusive interruption of his or her freedom than some of the more traditional techniques to which I have referred?

Sir David Omand: No, I don't think I would accept that. When you turn to part 2 of the Regulation of Investigatory Powers Act 2000, that, with appropriate warrants, allows the police or the Security Service secretly to enter your dwelling, to plant cameras and microphones, and to surveil

your most intimate activity. Such warrants would only, as I know from my own experience, be granted in the most exceptional cases, but Parliament has given that power, and that is much more powerful in the sense of potential moral hazard—not only to the suspect, but to all those who, quite innocently, might be in the suspect's dwelling—than intercepting occasional e-mails or the communications data on whom somebody was contacting. But I don't deny your point about metadata. In modern conditions, you can get more information if you are duly authorised.

Q6 Fiona Mactaggart: Some professionals—doctors, journalists, lawyers and so on—depend on security to be able to do their jobs properly. Are you confident that the existing protections set out in the code of practice on the interception of communications are adequate to protect their communications?

Sir David Omand: I will give you a qualified answer, because the key here is not what is in the Act, but what is in the code of practice that Parliament approved after the Act. The code is, I gather, due for updating, and has been due for updating for some years—I hope the Committee will encourage the Home Office to produce an up-to-date version. That is where I would expect to see an expansion of the current section, which says that if, inadvertently, GCHQ, for example, were to intercept legally privileged material, it is obliged, under the current rules, to inform the Interception Commissioner.

It is easy to see how you could then build on that, and given a recent case, journalistic communications might well fall under that as well. So you don't need to alter the Act to do that; you just need to define through the code of practice how such cases are to be handled. One could not put in the Act that a journalist's communications would never be intercepted, which would be to imply that no journalist ever engaged, quite independent of his or her journalistic activity, in any criminal activity—one could not imply that any more than one could for a Member of the Houses of Parliament.

Chair: On that cheerful note, we move to bulk interception, this being perhaps the most controversial issue we have had raised with us by a series of witnesses.

Q7 Dr Lewis: As the Chairman said earlier, most of the witnesses—virtually all of them—accept that there are limitations on the privacy of individuals and that targeted searches, provided they are properly regulated, are acceptable. What is far more contentious is the way in which the agencies engage in the bulk collection of communications and personal data. They describe this as a haystack in which they are searching for needles or, as they often say, parts of needles. Many of the people who have given evidence to us say that they regard the actual collection of the haystack itself as an unacceptable infringement of privacy, even though the agencies say that they are not free to search at random in it and that their searches are targeted according to specific criteria. Therefore, we want to know whether you have concerns about the collection of the haystack itself, or are such concerns mitigated by the fact that the searches carried out in the haystack are targeted?

Sir David Omand: I think there are a number of safeguards over what we describe as bulk access, one of which is that it does require a warrant that is actually limiting the nature of the bulk access. Attached to that warrant is a certificate, which specifies the nature of the material, if found, that can then be seen by a human being, so I think there are safeguards.

Most of the hostile legal opinions—if I can describe them as that—that I have read, including the recent one from Ben Emmerson QC, the UN rapporteur, create, as it were, a straw man of mass surveillance, and then go on to say that if this is being done through bulk interception, you have all these problems. But if you accept the premise, which I do but they don't, that, by discriminating and using computers to filter everything out, so that the only material that the human analyst—the sentient being—sees is that which is specified in the Foreign Secretary's certificate, you have got round the problem you would otherwise have of this wholesale plugging in of the computers.

To give a simple analogy, I make almost all of my financial transactions, when buying stuff, with a plastic card—now even a contactless card. Every single one of those transactions is run through the audit algorithm of my bank, so the most intimate details of everything I do go through that algorithm. From time to time, I get an automated e-mail saying, "Were you in Sweden? Did you really buy herring?" I will text back either yes or no. If it's no, the algorithm says, "This is prima facie fraud," so a human being gets to start to investigate and will ring me up. My card may have to be stopped and a new one issued because there is evidence of fraud. I have no objection whatever to the computer's algorithms running over that data, because I know that a human is only ever going to see anything if there is evidence of fraud. It is a rough analogy, but I don't think that, as the public, we should worry that there is computerised discrimination going on, if we can be assured—this is where Anthony May and the commissioners come in, with the inspections, and where your Committee comes in—that it is genuinely only the material the Foreign Secretary has authorised in the certificate that gets looked at and that the bulk access is not being used as some giant fishing expedition. Anthony May has assured us that that, indeed, is not what happens.

Q8 Dr Lewis: So what is your answer to those people who say the mere collection and existence of this bulk data is, in itself, an infringement of privacy? Do you think it would be a lesser infringement of privacy if the bulk data were, perhaps, to be held by the companies that originally collected it, rather than by Government?

Sir David Omand: I think that my answer to those critics is that, if this material was in the hands of an authoritarian Government who had no legal safeguards, no oversight and no Intelligence and Security Committee—I can think of several countries around the world that do bulk access and don't have any of these safeguards—yes, we would be right to worry. But if we have, as we have in the United Kingdom, law, regulation and oversight, my answer to the critics would be, "You don't need to worry about that. But there are some other things you should pay attention to." For how long is material being stored? I said in my written evidence that I was not a supporter of the idea, although it is technically possible, of hoovering up this material and keeping it for ever, just in case you might want to go back a few years and have a look. It seems to me that this is where "necessary" and "proportionate" come in. The Committee will no doubt want to talk to GCHQ about how long it keeps material for, but I think it is actually in accordance with "necessary" and "proportionate". Because they are a bit richer, our American friends tend to be a little more generous in that. The other point is that it is not possible for the computers to do online, real-time analysis of all the bulk data, and some kind of buffering—possibly for a day or two—may well be necessary while it is processed so that, out of the hopper, falls the wanted communication.

The other point that critics have made in my debates with them—I have had many of them—is that the certificate that the Foreign Secretary may sign is much more general than that of the 8(1) domestic warrant the Home Secretary signs. That is inevitable. Take the hypothetical example of Russian paramilitaries operating in eastern Ukraine. The European nations come together to impose sanctions on Russia. It is really rather important that somebody establishes whether those paramilitaries are not in touch with the Russian authorities and whether they are being guided. That is where communications come in, but you don't know who they are by name. You don't know what premises they are in, so an 8(1) warrant, you can't do. You are going to have to describe for the Foreign Secretary the purpose of the activity, why it's important, why it's necessary and why it would be proportionate to go trawling to try to find something. That is hypothetical; I have no idea whether they have been able to do that or not.

Q9 Dr Lewis: What about the companies, rather than GCHQ, holding on to the databases?

Sir David Omand: That could be a useful safeguard, and the United States has been looking at that for their interception. It is obviously cheaper for the Government—get the companies to do it, although you will have to subsidise them to do it. It doesn't necessary cover all the terrain. It could

be a useful adjunct, but I don't think it answers the full question, because the companies would not necessarily be able to hold them, and you would not necessarily have all the companies who are providing services that criminals, terrorists and so on are using able to do that.

Q10 Sir Menzies Campbell: I have a feeling I know the answer to the question I am about to ask from the tenor of what you have already said. It used to be said that that is the first rule of cross-examination. Some of those who have given evidence to us have said that it should be made clear in what circumstances an individual's communications may be read in the sense of publishing the criteria by which that decision would be taken. That might help an innocent member of the public, but on the other hand it might allow someone with more malign intent to take steps to try to avoid the coming together of these circumstances. Where do you stand on this matter?

Sir David Omand: I personally would find it quite difficult to frame such guidance. It clearly couldn't apply to external warrants just by the nature of life going on, and now you have jihadists going to Syria. How would you apply the criteria and would you be concerned about their privacy? If they are British citizens, you might say perhaps we should be, but will that apply to every intelligence operation in support of the armed services, the Taliban and so on? You would only really be talking about domestic interception under an 8(1) warrant signed by the Home Secretary.

The purposes set out in the Act are threefold: national security, the detection and prevention of serious crime and the economic well-being of the nation when that stems from an external cause, but there is a national security implication. Beyond that, you couldn't really say that these crimes fall in the basket and those don't. National security is notoriously difficult to pin down. It changes and the nature of the threats change. I would be very happy to look at a draft if someone produced one, but I am not sure I would know how to do it.

Q11 Dr Lewis: When pressed, critics of bulk surveillance argue that it is acceptable to pay the price, in terms of activities that are prevented by bulk surveillance not being prevented, to avoid the infringement of liberty that we discussed earlier. However, they tend to argue that, in any case, bulk interception is ineffective and they say that little evidence has been published to the contrary. So we have a dilemma because, as with everything secret, if the agencies publish examples of where bulk interception has been effective in generating leads and preventing terrorist outrages, for example, our enemies could learn from such disclosures and that would improve their ability to carry out attacks in future.

Do you have any thoughts on how to address this dilemma? Surely it would and should be possible to publish case studies and examples sufficiently far after the event which would show, if it is true, that leads obtained from bulk collection actually save lives.

Sir David Omand: The Home Secretary in her recent statement had a go at producing a justification, particularly of the communications data, and this was used in 95% of criminal cases, and so on. If you were to study the transcripts of terrorist trials, you would discover that although they can't be used in evidence, communications data are a very important investigative tool.

Q12 Dr Lewis: May I cut in for a moment? The critics would say with justification that in many, if not most, of those cases, the individual was already under suspicion and therefore was being targeted as an individual, and that the case isn't proven that, as a result of doing targeted searches of bulk collection, new leads have been generated.

Sir David Omand: Don't interpret this remark as flippant, because it is very seriously meant, but it is striking how the intelligence agencies—both MI6 and the Security Service—depend on GCHQ and the products of bulk interception. Given that GCHQ occupies the largest part of the intelligence budget, I have no doubt that if the intelligence agencies felt it is a waste of time, they would be the first to say, "Actually, I think we could use this money rather better than they could."

The same is true of the police—I know for a fact that SO15 relies on it. Were Parliament to decide that it is no longer going to be available, there would be consternation.

Q13 Dr Lewis: But you don't think we could give some more examples to the public of how it has worked?

Sir David Omand: It might be possible. Perhaps you could anonymise some of the examples. But there is a risk that you get drawn on it if people say, "Well, you have given that example. We are putting another case to you. Is this also possible?" Then you are on a slippery slope, and it will be increasingly difficult to protect certain things that you really don't want the people you are trying to intercept to know.

Q14 Chair: Do you think the effort might be worth making to see whether more information can be shared?

Sir David Omand: Yes, it is always worth having a look at that.

Q15 Chair: The public want to be reassured, but they want more than assurances: they want some basis on which they can accept those assurances.

Sir David Omand: One idea I have floated is the publication of some specimen warrants, which would clearly have to be carefully anonymised, so the public can see what the Foreign Secretary and the Home Secretary see—the details of the case and the careful legal analysis of whether it was proportionate.

Q16 Chair: We are examining that very suggestion at the moment, because we are also interested in that idea. Thank you. I am conscious that we have only about 15 minutes more. There are a number of other areas we would like to raise with you, so let us keep the questions short and get very specific answers. First, on the structure of the legislation, RIPA has been described as an "analogue law in a digital age"—you may have heard that phrase. Is there a case for reforming RIPA, or are you not concerned about that? Please answer briefly, if you could.

Sir David Omand: I don't accept the accusation that it is an analogue Act. To declare an interest, I was permanent secretary at the Home Office when it was passed, and I put a lot of effort into understanding it and the debates. We could see the internet developing—Hotmail existed, e-mails existed—so we had some idea. The whole idea was to make it technology-neutral. That is why, for example, we went for a very restricted definition of communications data. We did not want to have to keep coming back to Parliament every time somebody developed a new app.

I am perfectly open-minded, and if somebody produced a case for why it is necessary to amend the Act, I would be the first to support it. But it works well and Anthony May has looked at it. I can't see the parts of the Act that need new provisions. However, it is incomprehensible.

Q17 Chair: Was that deliberate?

Sir David Omand: I assure the Committee that it was not deliberate, but the parliamentary draftsmen found it very hard because it is a complicated Act. That is why in my written evidence I put the emphasis on the code of practice. Anthony May has done us a service by explaining in plain English how a lot of it works. Why on earth couldn't that have been done earlier?

Q18 Sir Menzies Campbell: One of the more controversial issues that has been raised with us in relation to 8(4) warrants is the suggestion that there is a lower threshold for intercepting overseas communications. What is your response to that?

Sir David Omand: That depends on how you are using the word "threshold". As I said, it has to be more general. It can't be the same as an 8(1) warrant, because you don't know the name of the Russian paramilitary, and you can't name a premise that the individual might be in—as you could if, for example, you had security service surveillance for a domestic warrant. Inevitably, you could say it is looser, but that comes back to whether the necessity and proportionality tests have genuinely been applied to the certificate that the Foreign Secretary has to sign to specify that it is not a general trawl, but that there is a specific reason why information is being sought. Some of it, of course, may be traditional, such as the air defence systems of certain countries.

Q19 Sir Menzies Campbell: You clearly have experience of application for and the application of those warrants. Have you ever had occasion to believe that the proper tests were not being observed?

Sir David Omand: No. You have the staff themselves in the intelligence agencies or in the police, but then you have, if you like, policy civil servants in the Departments scrutinising it.

Certainly, when I was PUS at the Home Office, I personally scrutinised most of the warrants going to the Home Secretary—there were fewer in those pre-9/11 days—and occasionally threw them back and said, "No, I am not putting this to the Home Secretary because you haven't really made the case." Then they would go away and mostly they would come back because it was just bad drafting and they hadn't done their homework. Very occasionally, they would come back and say, "Well, actually, perhaps we won't bother at the moment." The risk, of course, is that if you are too zealous in a type 1, type 2 error problem then you are going to screen out warrants that should have been signed and then something awful will happen.

Q20 Lord Butler: Do you think there is still a distinction between communications and metadata? Do we and the United States take different views of the definitions of those terms?

Sir David Omand: Yes, I think we do have a different definition. I don't think I have seen anywhere a definition of metadata in law, so it is a kind of term of general journalistic use. Very often included in it are such things as the address book on your phone, your entire internet browsing history and so on. Under UK law under RIPA that is content, not communications data. Section 21(6) of RIPA, which I have to confess is not an easy read, defines very narrowly what we in the UK are allowed to get as communications data. As the Act says, you do not need a Secretary of State's warrant to get communications data; there is provision for that. We felt, at the time, that we should restrict that to who called whom, when and where. All the fancy stuff that has emerged since is content.

Q21 Chair: Would you just be absolutely clear about this? Are you saying that, although the agencies that have authorisation to collect communications data could technically find out a lot more than purely who, where and when, by law in the United Kingdom they are not permitted to do that on the basis of the authorisation they have been given?

Sir David Omand: Unless they have an authorisation for content.

Q22 Chair: Indeed, unless they have the warrant. Are you saying that they are not allowed to do that, but that in the United States that distinction does not exist?

Sir David Omand: That distinction, as far as I am aware, does not exist there, at least not in the same way.

Q23 Chair: This is important. Much of the criticism on both sides of the Atlantic has been that communications data is not restricted in that way.

Sir David Omand: And of course that is one of the reasons why, when *The Guardian* started alleging that GCHQ staff were able simply to go to the United States and get the much wider class of data from their giant Dishfire database that they would not have been able to get here, that was not actually true. The analysts in GCHQ have to follow UK law. If they do not have UK authority, they have to get it before they get the material from the United States. The United States is very generous and helpful but, as I say, we have deliberately restricted in the Act what our own analysts can do. I am comfortable with that. Although you could make a case for saying that it would be better to abolish the distinction, actually I think it is a safeguard.

Q24 Chair: Some critics have said that in an internet age, when we use the internet so much, "who, when, where" gives far more information about people's private affairs than it used to. An example that is often quoted is if you constantly ring up Alcoholics Anonymous. Do you think that that is a valid point?

Sir David Omand: There is something in it. Even with old-fashioned telephones, people could infer something from the fact that you were calling Alcoholics Anonymous. The important point to register about the digital intersection and the internet is that the communications data definition only allows the analyst to know which computer has contacted which computer, not what then takes place. That is called interception up to the first slash in the internet address, so you can find out that the suspect accessed Google, but not the questions that they asked, because that is content. You can find out that they went on Amazon, but not what they bought, because that is content. This is in section 21(6) of RIPA, which says "data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored." It is not an easy read, but that is what it means.

Chair: In the last few minutes, we have some questions on oversight.

Q25 Lord Butler: You know the framework that activities of the agencies are warranted by Ministers and audited by commissioners, who are judges, and complaints are heard by a special tribunal. Do you think that that framework needs changing, and if so, how?

Sir David Omand: The framework, as I said earlier, is consistent with the guidance that you can derive from European Court of Human Rights judgments over the years, so you have got independent adjudication of complaints. You have got parliamentary oversight, which I think is rather important. The only point that I have been making is that self-regulation is the most important form of regulation, as anyone who has brought up a teenager knows. You can have all the rules and all the oversight, but when they are out of your sight, you have to rely on the fact that they have internalised a code of values.

How do we know that the managers of the intelligence agencies, whatever they may say to you, are actually behaving with the kind of integrity that I believe they have, and that they say they have? I think, frankly, that that is a job for your Committee, Chair, because you can eyeball them. You, as experienced people, can test "Are these people of integrity? Do they value privacy as a right? Are they careful about intruding on people's privacy only when it is genuinely necessary, or are they being a bit cavalier?" That, I think, is an underestimated function of oversight—to test the moral calibre of the people we entrust with these extraordinary powers.

Q26 Mark Field: As for the signing of warrants, in order to maximise public confidence, would you go along with the view that was expressed by some of the people whom we have spoken to that this should now be a matter solely for judges, rather than even the highest elected Ministers?

Sir David Omand: It is a very good question. One way of approaching it would be to try to distinguish between the law enforcement layer and the intelligence layer. The intelligence agencies

are Departments of State, and they are agents of the state, for which Ministers are accountable to Parliament. Therefore, I think it is entirely right that a Minister takes the responsibility on herself or himself to sign the warrant and then answers for the consequences if something terrible happens.

The police service is operationally independent of the Government—it is not part of government—so you could make a case for saying that a judge should do it. When you come on to communications data, there is a very large volume of requests for communications data from the police. They are almost all from the police, not from the intelligence agencies. You would overwhelm the system as it is presently organised, although that is not to say that you could not organise it differently. But I would be constitutionally disturbed at the thought that Ministers, who are accountable to Parliament, were not—in the last resort—taking responsibility for the use of these extraordinary powers that Parliament has provided.

Q27 Sir Menzies Campbell: Some people say we should have an inspector general. What do you think of that idea?

Sir David Omand: The phrase "inspector general" has been misunderstood in some quarters. If you look at the United States, the inspectors general are former members of the intelligence agencies and are performing internal audit, particularly of the giant agencies, so that the head of an agency has some idea of what is going on at the periphery. He can task the inspector general, who can do an internal audit job.

Q28 Sir Menzies Campbell: So they are not what one would describe as independent?

Sir David Omand: They are not the same as our commissioners at all. Now, you could have such people in addition to all the other things, but I am not sure that it would add more value than having someone like Sir Anthony May going in and looking at the books.

Q29 Fiona Mactaggart: Your evidence focuses clearly on the need for public confidence. Earlier you said that if you were trying to find out how this system operates, one clue is in the transcripts of trials where intercept evidence cannot be used, but you can see the consequences of it. Two questions arise for me out of that. First, do you think that intercept evidence ought to be able to be used in trials? Secondly, the IPT, which is the kind of final appeal, is a secret body. It rarely finds against the Government and it is not very transparent, so would you reform it?

Sir David Omand: To take the second point first, the IPT necessarily has to do most of its work in secret. I gather that, in its current case, it has had some hearings with the appellants' lawyers present, but most of it will have to be in secret, just because of the nature of the kind of cases it is looking at, particularly if it is looking at a complaint from a member of the public about whether they have or have not been put under surveillance. That is not something that you should have in public, so there will always be a slight problem about how you convince the public about that. Sorry, what was your first point?

Q30 Fiona Mactaggart: My first point was referring to your saying that one of the ways in which you can see how this operates is by looking at transcripts of trials where intercept evidence cannot be used.

Sir David Omand: I would be very much in favour of using intercept as evidence—I always have been—provided that somebody can come up with a scheme that does not cause more harm than good, and nobody has. I have been involved in three separate exercises in my time, and there have been others since, about trying to construct a legal system. They have tried different kinds of warrants—evidential warrants and intelligence warrants. Counsel's opinion was that that would collapse under scrutiny. They have tried the idea of the American-style separate court hearing on the

validity of evidence, and then you have the trial. They have thought about investigative magistrates, as one has in France, as a way of getting round this, but our legal system is not prepared to accept that in England, although one has, of course, the procurator fiscal in Scotland.

Nobody has found a system that accommodates the scale of activity that we need and the fact that we have incorporated the human rights convention into our domestic law, so that there will be challenges on human rights grounds. And we have an adversarial system, so the defendant has equality of arms—the right to see the material. You can imagine the fishing expeditions that would immediately take place, with people saying, "My client was under investigation, or was in contact with someone else," and that someone else may not know that they were under surveillance. So the moment you start tugging on that string, the jumper will unravel rather quickly. However, if you could find a way of doing it I am all for doing it, because it would help criminal trials.

Q31 Chair: Finally, on the question of transparency, you have offered the suggestion, which we are interested in, of anonymised warrants being made available to the public, so that they could see the process. Do you have any other suggestions about how transparency could be enhanced?

Sir David Omand: The most important thing is to explain how the system actually works and, as importantly, what it does not allow as well as what it does allow. The Act is no use for public presentation; it is just too complicated. The code of conduct is out of date and its language is not really that accessible. Anthony May's report is a great start but that, too, is written in very careful legal language.

I think that the task is for Ministers, from whatever party, to take the case to the public and, in particular, to dispel the illusion that has been created that we are under mass surveillance, because we are not.

Chair: Sir David, thank you very much indeed, both for your written submission and for the frank and open way in which you have shared with us your thoughts today. We are most grateful.

12:00

The session concluded