INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT

PRIVACY AND SECURITY INQUIRY

PUBLIC EVIDENCE SESSION 9

TRANSCRIPT OF EVIDENCE

Evidence given by:

The Rt. Hon. Philip Hammond MP
The Foreign Secretary

Sarah MacIntosh
Director General, Defence and Intelligence, FCO

Laurie Bristow
Director, National Security, FCO

Thursday 23 October 2014
(13:00 – 14:00)

Q1 Chair: May I welcome you, Foreign Secretary, to this public hearing of the Intelligence and Security Committee as part of our inquiry on privacy and security? Although the Committee has taken evidence from Foreign Secretaries on many previous occasions, this will be the very first time that it has done so in a public session. We are grateful to you and the two colleagues who are accompanying you. Simply so that they can be recorded, would your colleagues give their names and responsibilities?

Sarah MacIntosh: I am Sarah MacIntosh, director general for Defence and Intelligence at the Foreign Office.

Laurie Bristow: I am Laurie Bristow, director, National Security, at the Foreign Office.

Q2 Chair: Thank you very much indeed.

Foreign Secretary, as I think you are aware, the Committee has been conducting this inquiry into privacy and security, and all the associated issues relating to that. We have taken both public and private evidence. We have the privilege of your being here for an hour now, and we will subsequently go into private session for a further opportunity to put questions to you and your colleagues. Your evidence is being given after we have heard evidence from a wide range of

agencies, Ministers and members of the public, most of which has been in public session. Do you wish to make any opening comments?

Mr Hammond: It is a privilege to be part of such a historic occasion.

Perhaps I may start by saying that I regard the maintenance both of our security and of the privacy of our citizens as vital responsibilities of the Government. Getting that balance right is, of course, the challenge that we are all seeking to achieve. We face enormous numbers of threats from terrorism, cyber-attack, serious and organised crime, and the proliferation of weapons of mass destruction. We saw yesterday in Canada the need for vigilance as we go about our business. We are acutely conscious of the fact that the public mood on these issues will oscillate between a preference for privacy over security in times when our security does not seem to be immediately challenged, to a preference for security at all costs at times when we face great security challenges. Our job, I think, is to keep a level head through those oscillations, to get the correct balance between security and the protection of privacy, and to ensure that we adhere to what we have judged to be the right balance between those two paramount requirements for the Government to deliver to citizens. I hope that your inquiry will make a significant contribution to our understanding of how we are doing at getting that balance right.

Chair: Thank you very much for those opening remarks.

Q3 Dr Lewis: It has recently been suggested that even senior Ministers on the National Security Council have little idea about the actual work that the security and intelligence agencies do. Has assuming responsibility for GCHQ and SIS changed your perceptions of the work that the agencies do and, particularly, changed your views about privacy matters?

Mr Hammond: I understand the question but, if I may, I would like to answer it by referring to my appointment as Defence Secretary, because I think that the Defence Secretary, the Home Secretary, the Foreign Secretary and the Prime Minister probably have a slightly more detailed view of the work of the agencies, and certainly will have more of an understanding of the tradecraft aspects, as opposed to simply the outputs of the work the agencies do. Yes, I think it probably is true to say that when I was appointed Defence Secretary, and started to see material and to have an exposure to the agencies, I started to understand much more about how they work than I had done previously, and than some of my ministerial colleagues will understand. I have understood, as well, the very important judgments that need to be made when balancing privacy considerations against security considerations—essentially, when exercising the judgment about proportionality and necessity whenever intrusion into privacy is to be allowed. But I would say that I have also seen the incredibly important role that the work of the agencies plays in ensuring our security. Having that insight is clearly crucially important in making the judgments that Secretaries of State make in signing warrants and certificates.

Q4 Dr Lewis: Did the potential of the agencies to intrude on people's privacy come as a surprise to you?

Mr Hammond: No, I don't think it came as a surprise to me. What I've seen is the very careful safeguards that are in place, which are not just the legal safeguards, robust as they are, but the oversight safeguards. There are, as you will know, multiple layers—this Committee is one of them—of oversight of what goes on, but there is also a very important safeguard provided by the culture within the agencies, which is the exact opposite of what some movies might like to suggest. The agencies are extremely cautious, and extremely focused on their responsibility to maintain the culture of proportionality and necessity in everything they do. There is an atmosphere in the agencies that is very far from a gung-ho approach; it is very cautious and very measured, and that should be a great reassurance to us.

Chair: Thank you very much indeed. We would now like to move to more specific questioning on various aspects of the capabilities of the agencies, in so far as they relate to your responsibilities.

Q5 Lord Butler: Foreign Secretary, further to your reference to the oscillation of the public mood, do you think that greater intrusion into people's privacy is justified when the threat is greater?

Mr Hammond: Broadly speaking, I think that is right—over the long term. I don't think we should treat that as a reason to change levels of intrusion into privacy on a weekly, monthly or even annual basis, but looking at the level of challenge that we face today, and particularly the threat from terrorism, I think the mood of the public is that they want to be secure and that they recognise that a certain level of intrusion is required in order to deliver that security. Opinion polling consistently shows that the public recognise that there is a level of intrusion that is required, and that is proportionate and that is justified.

Q6 Lord Butler: In relation to your responsibilities, targeted intrusion within the UK is normally the responsibility of the Security Service and the Home Secretary. In view of your responsibility for GCHQ and SIS, which mainly operate overseas, could you tell the Committee whether there are any intrusive activities within the UK that you authorise SIS and GCHQ to undertake?

Mr Hammond: Section 8(1) warrants, which authorise intrusion against persons in the UK, are signed by the Foreign Secretary, so there are occasions when such warrants are necessary.

Q7 Lord Butler: The Home Secretary clearly has an interest in that. Is the Home Secretary consulted when you're signing a warrant for GCHQ under section 8(1)?

Mr Hammond: Not necessarily. She will be consulted when she will have an interest, and we talk regularly about matters, both domestically and externally, where we have overlapping interests and areas of responsibility. Some of the section 8(1) warrants that I will execute will not have any particular relevance to the Home Secretary, and I would not routinely discuss them with her.

Chair: Thank you very much. We now move on to perhaps one of the most controversial aspects of the work that we are doing: bulk interception by GCHQ and, whenever relevant, by others.

Q8 Mark Field: You will appreciate we have had quite extensive evidence sessions in recent weeks. It has been argued quite forcibly by a number of external groups that agencies do have a broad range of capabilities already and therefore do not need this bulk interception. How important do you feel that bulk interception is to the agencies and could they do without it?

Mr Hammond: Bulk interception is a tool that is at the heart of the agencies' ability to do what they do. I think Sir Iain Lobban has described it as building the haystack within which you can then search for the essential needle that protects our national security.

Being able to acquire data on a large scale and then filter it down—it is a very radical filtering process, and the overwhelming majority of data required will be discarded or destroyed immediately, or within a very short period of time—but does allow a series of filters and cross-references to be run automatically to identify that tiny element within the bulk data acquired that could be worthy of further analysis and filtering, and ultimately of review by a human pair of eyes. However, I should emphasise that it will be only a tiny, tiny fraction of bulk data acquired that will ever reach a human analyst.

Q9 Mark Field: But the development of that haystack, as GCHQ has described it, also leads to the overwhelming concern from a lot of civil liberties groups that somehow we are therefore open to

almost mass and indiscriminate surveillance. That particular phrase was used by several groups we have spoken to in recent weeks.

How would you respond to the allegation that, notwithstanding the fact that, much as you say, —anything other than a tiny amount—is discarded without seeing the light of day or the human eye, GCHQ's capabilities are never the less of deep concern to those who have a strong civil liberties bent?

Mr Hammond: I would reject the allegation that bulk data collection amounts to mass surveillance. There are two answers to the question. Does the ability to collect bulk data at least in theory provide the ability to carry out mass surveillance? The answer is in a country like ours, the answer is certainly not, for reasons of resource. It is impossible to conceive of the level of resource being made available that would allow even a tiny fraction of the bulk data to be analysed or used in any way. In other countries that devote very much larger resources of the state to surveillance, different considerations may of course apply, but in Western democracies, where the resources available are distinctly finite, there is a practical, technical reason why this should not be seen as a threat.

There is also, of course, a huge safeguard in the layers of rules, controls and oversight that are in place. Mass surveillance is illegal. It would always be illegal under our framework. There are strict rules in place to make sure that bulk data collected is not abused in any way. There is rigorous oversight to ensure that those rules are complied with. Even if it was practical—which it is not, for resource reasons—it would not happen, because it is illegal and the system is designed to prevent that kind of illegality occurring.

Q10 Mark Field: So your argument would be that not only do we absolutely not have mass surveillance, but we actually have highly selective surveillance, and that works both culturally and also, as you say, within the confines of pretty finite resources—

Mr Hammond: Absolutely right. As a citizen, my greatest reassurance is the resource one. It would be simply impossible even for the most intrusive state in the world, it would be impossible for that state to mass analyse the communications of individuals because of the sheer volume passing across the global communications system.

Q11 Chair: Some of our witnesses would not necessarily disagree with the facts that you have shared with the Committee, but have still argued that the very fact that large numbers of e-mails and other communications, most of which belong to perfectly innocent and respectable people, are collected and analysed, even if only by computer, is a significant intrusion on privacy. They argue that that ought to be unacceptable in a free society. How do you respond to that?

Mr Hammond: I would reject that notion. I think that the automated application of selection criteria by a computer and then the immediate discarding of 99.999% of the data collected does not give rise to intrusion. I would argue that intrusion arises at the point of the interrogation of data, not the point when it is simply collected and filtered according to an automatic process. I don't think that anyone has anything to fear from what, in many cases, will be the momentary acquisition of data before it is discarded as not having satisfied any of the criteria for further examination.

Chair: Julian, I inadvertently entered into your territory.

Q12 Dr Lewis: Not at all, Chairman; you enable me to take this a step further.

I want briefly to take issue with what you said about the reassurance that civil liberties groups, and indeed citizens generally, ought to have in the knowledge that, on the issue of sheer resource, you are saying, "This bulk data is so great that obviously we can't look at all of it." I am sure that critics of the collection of bulk data would not suggest for a moment that any state has the ability to

look at all of it, all at once, but what it does have is the ability to search through all of it in any way it chooses, unless legal constraints prevent it from doing so. While you say that the mere collection of the haystack should not be a matter of concern, although the civil liberties groups challenge that, surely the key point is how you direct your searches of the haystack, because you could just as easily direct them to a bad and unacceptable use as to the purposes for which they ought to be carried out.

Mr Hammond: That is of course true. In the case of the UK, we have very strict protocols and procedures in place, and the criteria for the filtering and selection of data for further analysis are set out in the warrant, so as well as having to operate within the legal framework, political judgment is exercised by the Secretary of State when authorising such bulk data collection to ensure that the filters that are used are appropriate. The question that I ask myself is not just are they necessary and proportionate, which they must be for the action to be lawful, but would they stand the test of public opinion: if the public were able to see the criteria used and how the work was being done, would they accept that this was a reasonable and proportionate thing for us to do to keep them safe?

Q13 Dr Lewis: So you are saying that if I was a rogue agent in one of the agencies and I had this pool—this haystack—there would be no way I could abuse that by searching for something that I shouldn't search for.

Mr Hammond: That is correct, and I am drawing now not on my briefing, but on something I remember, because I asked precisely that question when I visited GCHQ. There are, in fact, technical protections in the system to prevent someone who is authorised to access the system from using it in a way that would be abusive.

Q14 Chair: I think that the United States might have thought that they had such technical methods of preventing that from happening, but sadly they didn't work. Do you think that you can be satisfied that the methods available to GCHQ are in fact effective?

Mr Hammond: If you are referring to the Snowdon case, what happened, of course, was that data was stolen. I think the question was specifically about whether the selection criteria, which are carefully defined and subject to political as well as legal judgment, could be ignored by an agent with access to the system and replaced with different selection criteria. We have seen over time that we have very robust processes in place to prevent that from happening and to identify any attempted abuse of the system.

Q15 Lord Butler: May we pursue the issue of the selection criteria for a moment? The powers under RIPA and section 8(4) to collect overseas intelligence are very wide. Those are then narrowed down by a warrant signed by the Foreign Secretary that limits the selection to certain categories. Can you tell us anything about how many categories there are and how tightly drawn they are, and perhaps even give us an example of the sort of category there would be? For example, in present circumstances, might it be every e-mail sent from Syria? Or would it be a narrower definition?

Mr Hammond: That might be a subject we might discuss further in the closed session.

Q16 Lord Butler: Certainly; I quite accept that. I just wondered whether there was anything you could say in open session that would reassure the public about the narrowness.

Mr Hammond: Whether it will reassure the public, I cannot say. All I can say is that we are acutely conscious of the need, for a variety of reasons—public reassurance and proper application of political control, but also resource constraint—to define criteria as narrowly as possible. If you think about it, given the limited resource available, if we define the criteria too widely, we are blunting the surgical instrument that we are seeking to use, and that would absolutely not be in the interests of what we are trying to achieve. What I do not want to do is to give any pointers in open session to the

type of selectors that we would use because we have seen already that when information comes into the public domain that allows people to identify any aspects of the tradecraft used, they will modify their behaviour accordingly, and that makes us less safe and the agencies less effective.

Q17 Lord Butler: That is understood. In the United States, the National Security Agency has given some figures about the extent to which the mass material it collects is filtered down. The figures that I have are that the NSA has stated publicly that it collects 1.6% of internet traffic, which is of course a very large volume, but examines only 0.00004%—I think I have that right—of what is picked up. Can any similar figures be given publicly for what GCHQ picks up in order to dispel the fear that people have of mass intrusion?

Mr Hammond: I do not think that I can give any figures in the public session, but I can give more information in the closed session.

Q18 Chair: I hope that you will also be able to explain in the closed session why you are unable to give these figures publicly if the United States does not appear to have such an anxiety.

Mr Hammond: Perhaps I could make a general comment. Just because something has come into the public domain about how the United States does things, it does not necessarily mean that we think that having that information in the public domain is conducive to optimising our national security.

Q19 Chair: If I am not mistaken, the United States' NSA itself announced the figures, but we will have to check that.

Mr Hammond: That is for them to decide.

Chair: Indeed, it is their own decision.

Q20 Dr Lewis: Chairman, I know you are always very strong on pithy questions, but this one has four elements.

Chair: I appreciate that.

Dr Lewis: I look to the Chair's indulgence.

This is all about the distinction between regarding communications as internal to the UK or external. This is obviously important because there are tighter restrictions on examining internal communications than there are on external ones. For that reason, the Regulation of Investigatory Powers Act—the legislation—draws this distinction. In the past, it was quite easy to interpret what was internal and external, so a letter posted overseas, or an international telephone call, was self-evidently an external communication, but this is much harder in certain areas to do with internet activity. So, I have my four examples, which I hope you will help me navigate.

First, in terms of an e-mail, it is obvious that if one or both of the sender and the recipient is overseas, that would be an external communication, but can you confirm that if both the sender and the recipient are in the UK, it will always be treated as an internal communication, even if it is routed overseas during its journey? Could we look at that one first, please?

Mr Hammond: You said an e-mail.

Dr Lewis: An e-mail from me to you. We are both in this country, even though, as a result of the arrangements, it may have bounced back and forth with servers overseas.

Mr Hammond: I invite my colleagues to step in if I get this technically wrong, but I think you are absolutely right, Dr Lewis, to identify that because of the technology that exists, these issues have become more complicated. An e-mail that originates from or is received in the UK, whether both parties are in the UK, or only one of them is in the UK, is an internal e-mail. It is however the case—

Q21 Dr Lewis: I don't think that that can be right—not if only one of them is in the UK.

Mr Hammond: I think it is in terms of the access to its content would require a warrant under section 8(1).

Sarah MacIntosh: If both ends of the e-mail are in the UK, it is treated as an internal communication.

Q22 Dr Lewis: Yes, but that is not what the Foreign Secretary is saying.

Mr Hammond: But if only one end is in the UK, it will still require a section 8(1) warrant to access the content.

Q23 Dr Lewis: Yes, but that is an external communication.

Mr Hammond: Let me finish the train of thought and then, if I am being unclear, I will correct myself.

My understanding is that because of the technical nature of the internet, it is possible, in either case, that such a communication could be routed through servers that are outside the UK. It is possible that data so routed could be intercepted as a result of a warrant under section 8(4), but it would not be possible for that communication to be examined or analysed without a section 8(1) warrant then being issued, because the persons involved, or one of the persons involved, is in the UK. If I have misrepresented that, please correct me.

Q24 Dr Lewis: Yes, but the point I want to establish is that different warrants allow different levels of intrusion, and you do need to have warrants of one sort to deal with external communications—from somebody within the UK to somebody outside it—but if that person is communicating with somebody within the UK, that is regarded as an internal communication and requires a different sort of warrant.

Mr Hammond: My understanding is that a section 8(4) warrant will allow external communications—those which are between two parties outside the UK—

Sarah MacIntosh: Or one party outside the UK.

Mr Hammond: Or one party outside the UK.

Sarah MacIntosh: It is external if one party is outside the UK.

Mr Hammond: Okay. Then that requires a section 16(3), if the content is to be examined.

So for practical purposes, the point I am trying to make is that, through a combination of the use of section 8(1) warrants and section 16(3) warrants, it is the case that however it is originally collected, if an e-mail has a party to it—either the recipient or the sender—who is in the UK, it will require a further warrant to be issued, either a section 8(1) or a section 16(3), before that e-mail can be examined. If it is an e-mail passing between persons who are both outside the UK, it could be examined under the authorities granted under the section 8(4) warrant. That is not an open-ended right to examine that e-mail—the section 8(4) itself will define the filters that have to be applied for the examination of such an e-mail.[1]

[1] *The Foreign Secretary clarified after the meeting that, if a communication is intercepted under an s.8(4) warrant, and if one end is outside of the UK, it may be selected for examination without a 16(3) modification if the subject of interest is the non-UK end of the communication; however, if the subject of interest is the party in the UK, or if both ends are UK, there needs to be a 16(3) modification or 8(1) warrant authorised by the Secretary of State before it can be selected. He undertook to write to the Committee with further detail.*

Q25 Dr Lewis: So, as I understand it, you are saying that an internal communication applies not only if both the sender and the recipient are within the UK, but even if only one of them is in the UK.

Mr Hammond: Sorry, I have misled you in my use of terms. I was trying to be helpful, but I fear that I have been unhelpful. It is an internal communication if both the sender and the recipient are in the UK. If one of the sender or recipient is in the UK, it is an external communication but, because one of the sender or recipient is in the UK, a section 16(3) warrant will need to be issued before that communication can be examined.

Q26 Chair: Just to be clear, I think a 16(3) is described as a modification, rather than a new warrant.

Mr Hammond: That's right.

Q27 Dr Lewis: You will be pleased to know that that was the easy one; let us now move on to browsing the internet. If I read the website of *The Washington Post*, I am deemed to have communicated with a web server that is located overseas. Is that therefore an external communication according to the existing legislation, even though all I am doing is looking at a website that happens to have been posted and published abroad?

Mr Hammond: My understanding is that that would be an external communication but, again, because one of the parties to it is in the UK, it would require what the Chairman rightly described as a modification to be made in order for the content of that activity to be examined.

Q28 Dr Lewis: I suspect that your answer will be the same for the third example, which is particularly controversial: the case of social media. In recent evidence to a tribunal, Charles Farr from the Home Office caused some anxiety by suggesting that Facebook posts are external communications. Can you clarify the situation? I am not, of course, talking about posts that are made on Facebook with no restrictions, because obviously they are available for all to see. However, if I were to post something on Facebook and had adjusted my settings with the intention that it should be read by only a restricted group of my friends, and if—this is the key point—all those friends were based in the UK, surely that should be treated as an internal communication rather than an external one?

Mr Hammond: I think it is the case that if you post something on Facebook and the server is outside the UK, it will be treated as an external communication. However, as I said in answer to my last question—you suspected I would say it in answer to this one, which I think means that we are making progress in understanding this—it would require the issue of a modification under 16(3) to enable the agencies to look at the content of that activity, because one of the parties to it was in the UK.

Q29 Dr Lewis: And if neither party was in the UK, a lesser level of authorisation would be required to look at it.

Mr Hammond: That is correct. The authorisation that was already attached to the section 8(4) warrant would define the circumstances in which the content could be examined.

Q30 Dr Lewis: So you are saying that, actually, it is not the end of the world by any means if something is classed as an external communication, even though one or both of the sender and recipient are British citizens in the UK, because that very fact will trigger a further safeguard to ensure that it is not examined any more freely than if it had been classed as an internal communication. Is that the argument we are hearing?

Mr Hammond: That is exactly the case, although I should be clear that it is not about being a British citizen, because the system is blind to citizenship and nationality. It is about where you are when the communication takes place. If you are in the UK when the communication takes place, then if both of you are in the UK, a section 8(1) warrant will be required, and if one of you is in the UK and the data is acquired under a section 8(4) warrant, authorisation to access that data would require a modification under 16(3).

Q31 Dr Lewis: I think that deals with the final scenario, but just for the sake of the record, let's just mention cloud storage, where no other person is involved at all. It may be my decision to upload photographs into Dropbox or a lot of private information into the cloud generally. Would those communications still be regarded as external because they had been sent to a web server overseas, or would they be internal because the only person with access to them is me and I am here in the UK?

Mr Hammond: If the server is overseas, they will be regarded as external and they will be subject to the same safeguards as an e-mail sent by a UK person to a person overseas.

Q32 Dr Lewis: Just for completeness, if I am somebody whom you are interested in from the point of view of national security, would I have the same assurance of security for something I had uploaded to the cloud externally but then the modification kicked in before you examined it as if I had uploaded it to a server in the UK and you used the other form of warrant directly? In other words, with the two types of warrant, one is looser than the other, and when you take the looser type of warrant and add the modification, is it as strong as the tighter form of warrant?

Mr Hammond: Yes, it effectively turns the 8(4) process into an 8(1) process. It looks very similar and the same considerations will be presented in delivering the modification to the Secretary of State.

Dr Lewis: That is extremely clear. Thank you.

Q33 Chair: To conclude this area of discussion, may I ask you a particular question? It clearly is a very complex issue. You have given very detailed replies and the Committee has noted that. There is a lot of public concern as to the perception of different levels of safeguard, depending on whether it is internal or external. Is there not a case for the Government authorising that we should try to draw up some document in language that could be understood by the wider public as to the difference between internal and external, and setting out when one applies and when the other applies, and the rationale behind it?

Mr Hammond: What people in the UK need to understand is that the communications of people in the UK will be examined only on the basis of a specific authorisation by a Secretary of State, either under section 8(1) or by the issue of a section 16(3) modification, where the data has been acquired under an 8(4) warrant. They should be clear about that and that they enjoy that protection as a result of being in the United Kingdom, even when they are using an external, overseas server, or communicating with someone who is outside the UK.

Q34 Chair: It is helpful that you have made that statement in public session today, but it is still in fairly formal language. I am not asking for a decision today, but is it not worth considering whether some document could be published by the Government, GCHQ or whomsoever that would explain and give examples of the kind that Dr Lewis put to you as to how the answer points in the direction that you have indicated?

Mr Hammond: I am certainly prepared to look at it, or might I perhaps even suggest that the Committee draws attention to that in its report?

Q35 Chair: We can do that, but we are not the Government, and it is the Government, or the agencies, that come under criticism. If it is worth doing, it is worth doing in the name of the Government.

Mr Hammond: I will certainly look at whether I can say in simpler English what I have just said by referring to the different sections of the Act.

Q36 Chair: Thank you. I have a final question in this category. If you authorise GCHQ to examine external communications that it has gathered, would you expect that information to be used solely by GCHQ, or would you have any problems or difficulties if it passed some of the information to MI5 or the police for use in their domestic work?

Mr Hammond: GCHQ will be tasked to provide information to the other agencies. It works very closely, obviously, with the Secret Intelligence Service and with MI5, and now with the National Crime Agency as well, so it will, where appropriate, pass information to those agencies.

Q37 Chair: Thank you very much. Is there something you would like to add?

Sarah MacIntosh: Only to add that the information reports that support the whole of Government are of course available to all the agencies, but there are also requirements for individual agencies to have a need to know, based on their requirements, their statutory functions that they are fulfilling. So they cannot access information from GCHQ simply because they would be interested in it. They have statutory functions and a requirement to know, and that case must be made.

Q38 Chair: But that does imply that GCHQ, at least to some degree, has a domestic role, not just an overseas role, albeit that is a very modest proportion of its overall concerns.

Mr Hammond: I think the point is that the data are gathered primarily overseas. Other agencies—for example MI5, the Security Service—will clearly have an interest in data relating, let's say, to a putative terrorist plot affecting the United Kingdom.

Chair: Thank you. Let us now move to the legislation that governs the work of the agencies.

Q39 Lord Butler: An argument has been put to us that one of the ways in which the internet has changed the world is that, because we use it much more, many aspects of personal information are now available through the internet—it has grown hugely—and that in itself justifies greater protection. Do you think there is any validity in the argument that the internet has changed the world in which we ought to offer privacy to our citizens?

Mr Hammond: Well, it's certainly changed the world, and I guess it has meant that more data is generated because more data is usable. I suspect—well, I don't suspect, I know—that, in the past, there have been vast amounts of data, but that hasn't been readily accessible, except with the expenditure of huge amounts of effort trawling through paper files in records offices and things like that. The fact that much of this data is now available in a sortable and readily accessible form clearly feeds the appetite for still more data. People aren't demanding that more data be made publicly available when they don't have the resource to access and search it. Now that they can access and research it easily, that clearly drives the demand for more.

Q40 Lord Butler: A particular aspect of this is that the amount of communications data available through the internet tells more than it did about people's personal situations. We had evidence from Sir David Omand this morning that, none the less, the definition in RIPA of what constitutes communications data is very tight in this country—much tighter than in the United States—and that that still offers a degree of protection. Are you satisfied that our definition of

communications data is sufficiently tight to prevent intrusion into what is content about people's lives?

Mr Hammond: Yes, I am quite confident about that. I think that communications data are hugely important to establishing networks and patterns, but the protections around the use of communications data certainly provide a robust safeguard. As to content, that is a separate matter, dealt with separately.

Q41 Lord Butler: And dealt with by Ministers.

Mr Hammond: And dealt with by Ministers.

Lord Butler: Whereas communications data, of course, is not.

Mr Hammond: Let me just go back to the previous conversation. Of course, under section 8(4) warrants, content is dealt with by Ministers, but it is dealt with by Ministers on a class authorisation basis, rather than an individual case authorisation basis, for outside the UK.

Q42 Sir Menzies Campbell: As you know, Foreign Secretary—indeed, your own evidence this afternoon has reflected this—the majority of the debate about statutory provision is centred around RIPA. But, of course, there is other legislation, such as the Intelligence Services Act, which does allow for intrusion. In the spirit of transparency, do you think it would be sensible for the Government to make clear the extent to which authorisation can be obtained under the Intelligence Services Act?

Mr Hammond: To go directly to the role that I have in the issuing of warrants, principally under sections 5 and 7 of the Intelligence Services Act, I am clear that, in issuing a section 7 warrant, it is specifically limited to actions that take place outside the United Kingdom. Warrants are issued only if they are necessary and proportionate to protect agency operatives in carrying out the work that they do. I suspect that the public would be surprised and reassured to understand the level of authorisation that is required even for an agency operative in a foreign country even to carry out what might seem really rather trivial tasks. There is still a high level of authorisation required under the legislative framework.

Q43 Sir Menzies Campbell: So I think the answer to my question is yes-plus. Is that right?

Mr Hammond: You will have to remind me of the original question.

Sir Menzies Campbell: The point I am making is that the public debate has centred on RIPA. We have just discussed the Intelligence Services Act. In the atmosphere of transparency that I think we are all trying to create, consistent with the public interest and questions of security, I am suggesting to you that perhaps a little more disclosure by the Government of precisely what is capable of being authorised under the Intelligence Services Act might help to contribute to transparency.

Mr Hammond: If I may say so, I think that what is capable of being authorised is pretty clear from the Act and is, of course, a piece of public information. What is more important is that the regime of not merely legal control and authorisation, but political control and layers of accountability, means that what is authorised in practice sits well within the parameters of what could be authorised under the terms of the Act. People like myself who exercise ministerial control, and people like yourselves who oversee the process and exercise democratic accountability to Parliament, will tend to want to interpret narrowly the permissions that the Act gives and, as I mentioned earlier, apply the test of whether this would look and feel right if our constituents were aware of it. The way I want to work is such that I know that what I am doing, if I were able to explain it to a panel of open-minded constituents, would have them nodding in agreement that it was a sensible, reasonable and proportionate thing to do to protect our national security.

Sir Menzies Campbell: That is a very interesting illustration of how you see your responsibility, and I don't think it is one that we around the table would quarrel with.

Q44 Dr Lewis: This is our James Bond 007 moment, Foreign Secretary, because section 7 of the Intelligence Services Act has been described as the James Bond clause as it seems to provide what they would call MI6, and what we call SIS, with broad permission to do whatever it deems necessary. The relevant sentence, which I put on record for the benefit of the people watching this, states: "If, apart from this section, a person would be liable in the United Kingdom for any act done outside the British Islands, he shall not be so liable if the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State"—that is yourself—"under this section." How do you reassure the public here that SIS is not intruding unnecessarily into the private lives of individuals—they could of course be British individuals if so much of their data is stored in another country—under the broad cover that section 7 of the Intelligence Services Act provides?

Mr Hammond: The answer is that although the scope under the Act is broad, the warrant that is required—this is the Secretary of State's role—will define the actions that SIS will be allowed to carry out under that warrant. This Secretary of State will not be signing a warrant that says, "SIS named agent X can do whatever he likes in country Z." It will say, "X is authorised to carry out the following actions during the following time period, for the following purpose, in country Z".

Q45 Dr Lewis: There seems to be a common theme here with the haystack we were talking about before and how it is searched, in that you are saying that while it is true that the Secret Intelligence Service and GCHQ have these capabilities, the safeguards on them not abusing those capabilities are determined by the warrantry that is signed and the authorisation of the limits.

Mr Hammond: No, I think it is more reassuring than that. The Act gives the Secretary of State the power to render legal an act that, done overseas, would otherwise be illegal. That is the legal framework—a wide power to the Secretary of State.

The Secretary of State's democratic accountability, including through this Committee, ensures that that power will be exercised with great discretion and that individual authorisations will be narrowly defined. Indeed, as a matter of working practice, all the ones that I have seen are narrowly defined in the application for such warrants, and sometimes further restricted by the Secretary of State in the granting of the warrant.

Q46 Chair: Surely, with regard to this particular matter, it is not so much this Committee but the intelligence services commissioners who have the retrospective right to examine the individual warrants and how they were actually used.

Mr Hammond: They do. They have the right to examine the warrants, to understand how they were used, and to look at the advice that was given and any additional restrictions that were applied.

Q47 Fiona Mactaggart: There is another responsibility in the ISA on the director of GCHQ and the chief of SIS to ensure that information is disclosed where it is "necessary for the proper discharge of…functions". That seems to me to allow them to share information internationally with whoever they want. That has led to criticisms from groups such as Privacy International, which says specifically that this power should be codified in statute, and that these arrangements with overseas partners are too vague and do not provide adequate assurance that data shared with them is treated with the same privacy standards that we would expect in the UK. Could such arrangements be codified in statute or made publicly available?

Mr Hammond: I am just contemplating whether that is a question better answered in the closed session, if you wouldn't mind.

Q48 Fiona Mactaggart: May I ask this question, then? Do you believe it would be possible to make arrangements codified in law? I don't think there is anything secret about asking that.

Mr Hammond: "Possible" is a broad term. I guess it would be possible; the question is the extent to which it would impact on the effective working of the agencies. I am confident that we have robust arrangements in place to avoid the kind of abuse that you are speculating could occur, and I completely understand why you are. Whenever we pass data, how do we ensure that it is dealt with with the same degree of rigour and discretion that I have described here? I am confident that we have those arrangements in place, and particularly that data originating from persons in the UK is not vulnerable to any risk in that regard. If I may, I will elaborate further in the closed session.

Q49 Fiona Mactaggart: May I ask one more theoretical question? Do you accept that public confidence in the security of data would be enhanced by greater public understanding of what those arrangements might be?

Mr Hammond: The problem we have is that our relationships with other agencies outside the UK, which are critical to the maintenance of our capability, are relationships of trust. However much we might wish to be more transparent about those relationships, we can be so only if there is a similar willingness at the other end of the pipe, so we have to be extremely careful about how much we talk about our relationships in open session.

Chair: I am afraid that we have only some seven or eight minutes left of this public session, so can we move briefly to authorisation and accountability, Fiona?

Q50 Fiona Mactaggart: You have responsibility for authorising the activities of GCHQ and SIS. Most of the people whom we have spoken to during this inquiry say that judges should sign warrants, not you. What is your response to that?

Mr Hammond: I think that is wrong; I think it is a flawed analysis. I think the system would be weaker if judges signed warrants, because judges—quite properly—would look at the legal permissions and judge within those legal permissions. Secretaries of State, of course, are constrained by the legal permissions and will only exercise their powers on the basis of clear legal advice about how they can do so, but also apply a layer of political judgment, which is crucially important.

Most of the difficult warrants—most of the warrants that take serious time and consideration—are not debates about whether something is legal or not. Nothing should ever get to the Secretary of State with an open debate about whether an issue is legal; that will have been sorted out long before. By the time it gets to the Secretary of State, it is a question of political judgment. Is the benefit to our national security—to the safety and well-being of our citizens—justified by the political risk of the specific action being proposed? While judges, as intelligent, thoughtful people, would be able to have an opinion on it, in a democracy it has to be a democratically accountable person that makes such a decision, properly overseen by all the tiers of oversight that we have in this country.

Q51 Fiona Mactaggart: On those tiers of oversight and the commissioners who do that oversight, post hoc, we have had many arguments saying that they should be reformed or replaced by a new system. Are there any changes that you would like to be made in the commissioner system?

Mr Hammond: I think the system that we have in place works, and works effectively, but I think we should go on challenging it; we should go on asking the question, as I am sure you will, and making sure that it is robust. I think the way it works at the moment, with a mixture of politically accountable and judicially experienced oversight, is a very effective combination.

Anecdotally, but I will say it anyway, my experience is that wherever I go in the world as Foreign Secretary, or previously as Defence Secretary, and explain to colleagues the degree of direct,

hands-on, ministerial involvement in the process, they are astonished by the level of hands-on ministerial responsibility. In most systems internationally, there are far greater levels of delegated responsibility. I think we have a very, very tight and effective system here, which ensures that we operate within the law but with proper political judgment and full democratic accountability.

Q52 Sir Menzies Campbell: I am going to ask rather an optimistic question, Foreign Secretary. You have been Foreign Secretary for three months. Would it be damaging international security if you told us how many warrants you have authorised in that time, and how many operations GCHQ and SIS have carried out in that period?

Mr Hammond: Yes, I am afraid it would.

Q53 Sir Menzies Campbell: In that case, let me take refuge in a bit of pragmatism and ask you to describe, if you will, the scale of the warrants and the scale of the operations, because I think, again, that this is a matter that will make a contribution to public understanding and public accountability, not least of course in the light of the events in Canada in the last 24 hours.

Mr Hammond: I can say, for purposes of public reassurance, that our agencies are in close contact with their Canadian counterparts and, as you would expect, are already analysing what happened in Canada and the implications for us.

I cannot say anything about the scale of operations that I have authorised because almost by definition they are ongoing operations, but if it would help in terms of where your line of questioning is seeking to go, I will expect to spend several hours in each week considering warrants and reading the supporting paperwork, questioning officials about the material that I have received, and meeting with heads of agencies, or other senior people in the agencies, to discuss either specific issues or issues of broader policy that have arisen from warrant applications that I have received.

Chair: Thank you. Finally it is Robin, on transparency.

Q54 Lord Butler: Foreign Secretary, you have been understandably cautious this afternoon about what you have been prepared to say in public. The outgoing director of GCHQ, Sir Iain Lobban, told this Committee that he is "not evangelically opposed to publishing information about GCHQ's internet collection capabilities", but he went on to say that he would "need to get ministerial backing for this". Sir Iain's attitude is a conversion on the road to Damascus; he did not start in that position—

Sir Menzies Campbell: And he is about to leave.

Lord Butler: He may be demob happy. Subject to the advice of technical experts such as the director of GCHQ, are you in favour of increasing transparency in the activities of the intelligence agency?

Mr Hammond: Generally, I am confident, from what I have seen, that the public would be reassured by knowledge of the way the system works. Against that, we have to balance the indisputable fact that knowledge of how the system works allows those who have something to hide to adjust their behaviour. We have seen it since the Snowdon revelations: al-Qaeda senior operatives changing the way they communicate, and criminals operating over different communication routes. So we have to balance the self-interested desire to be able to be as transparent as possible in order to secure public reassurance against the reality that, if we expose tradecraft, it will cause behaviour change by those who are seeking to do us harm.

Q55 Mark Field: In your early weeks as Foreign Secretary you had a little encounter with the whole issue of "neither confirm nor deny" in relation to events. We have touched on the disparity, since the Snowdon revelations, between the reaction of the US and European Governments and that

of our own. There has been some criticism that we have been less willing to level with the public. Do you really think that the maxim of "neither confirm nor deny" will be tenable in the longer term?

Mr Hammond: Before I answer that, may I supplement my previous answer? I have been reminded that under the DRIPA legislation a new annual transparency report will be available.

"Neither confirm nor deny" is a vital part of our armoury. It is a self-denying ordinance; sometimes it is very tempting to reassure by denying, but if we once succumb to the temptation of reassuring by denying, the next time we neither confirm nor deny, we will have implicitly confirmed. We have considered this on a number of occasions very carefully, but maintaining "neither confirm nor deny" is an essential part of protecting what the agencies do and maintaining their ability to continue doing it.

Q56 Dr Lewis: You have repeatedly stressed the robustness of the legislation as a protection of, and reassurance to, the public. Can I just read you an extract from RIPA? It states: "Intercepted material also falls within subsection (2), notwithstanding that it is selected by reference to any such factor as is mentioned in paragraph (a) and (b) of that subsection, if…the person to whom the warrant is addressed believes, on reasonable grounds, that the circumstances are such that the material would fall within that subsection; or (b) the conditions set out in subsection (5) below are satisfied in relation to the selection of the material." That may be very robust legislation, Foreign Secretary, but do you not agree that to the ordinary member of the public it sounds like gobbledegook? Can we not get some legislation enacted that ordinary people can understand, so that they can be reassured?

Chair: Not even extraordinary people could understand that.

Mr Hammond: I think that question could be applied much more widely than to the intelligence services legislation. I suspect that most legislation is impenetrable to members of the public. All members of the Committee will know from their work as Members of Parliament that, because legislation is amended repeatedly over time, even reading the original legislation seldom gives a good guide to how it is operating currently.

Although you read out that quote rather quickly, the key point in there, which I have already made once, is that while the legislation provides a robust framework, it is about the reference to the person authorising the warrant. They are the ultimate safeguard: a person who is democratically accountable through parliamentary processes exercising political judgment. In practice, that political judgment will invariably be exercised some considerable way inside the parameters of what the law will allow, to ensure that the agencies are narrowly focused in what they seek to do on any operation.

Perhaps it is a feature of the times we live in, but I am sure I can speak for all my colleagues who sign warrants in saying that we all have in the back of our minds that at some future point we will—not might, but will—be appearing before some inquiry or tribunal or court, accounting for the decisions we have made and, essentially, accounting for how we have applied the proportionality and necessity tests. There is a very strong political incentive in this issue to apply the tests narrowly and in a way that minimises the scope of the agencies to interpret the warrants that are issued.

Chair: Thank you. You might even be appearing before this Committee on exactly that basis. Thank you very much for your very full and frank answers. We will adjourn and meet again in a closed session later this afternoon.

14:00

The session concluded