Made on behalf of: the Respondents
Witness: Charles Farr
Statement number: 1
Exhibit: CF1
Dated: 16 May 2014

IN THE INVESTIGATORY POWERS TRIBUNAL — Case No. IPT/13/92/CH
BETWEEN:

PRIVACY INTERNATIONAL

Claimant

and

(1) THE SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS
(2) THE SECRETARY OF STATE FOR THE HOME DEPARTMENT (3) THE SECRET INTELLIGENCE SERVICE
(4) THE SECURITY SERVICE
(5) THE GOVERNMENT COMMUNICATIONS HEADQUARTERS
(6) THE ATTORNEY GENERAL

Respondents

IN THE INVESTIGATORY POWERS TRIBUNAL — Case No. IPT/13/77/H
BETWEEN:

LIBERTY

Claimant

and

(1) THE GOVERNMENT COMMUNICATIONS HEADQUARTERS
(2) THE SECRET INTELLIGENCE SERVICE
(3) THE SECURITY SERVICE

Respondents

IN THE INVESTIGATORY POWERS TRIBUNAL — Case No. IPT/13/168-173/H
BETWEEN:

(1) AMERICAN CIVIL LIBERTIES UNION
(2) CANADIAN CIVIL LIBERTIES ASSOCIATION
(3) EGYPTIAN INITIATIVE FOR PERSONAL RIGHTS
(4) HUNGARIAN CIVIL LIBERTIES UNION
(5) IRISH COUNCIL FOR CIVIL LIBERTIES
(6) LEGAL RESOURCES CENTRE

Claimants

and

(1) THE GOVERNMENT COMMUNICATIONS HEADQUARTERS
(2) THE SECRET INTELLIGENCE SERVICE
(3) THE SECURITY SERVICE

Respondents

IN THE INVESTIGATORY POWERS TRIBUNAL — Case No. IPT/13/194/CH
BETWEEN:

AMNESTY INTERNATIONAL LIMITED

Claimant

and

(1) THE SECURITY SERVICE
(2) THE SECRET INTELLIGENCE SERVICE
(3) THE GOVERNMENT COMMUNICATIONS HEADQUARTERS
(4) THE SECRETARY OF STATE FOR THE HOME DEPARTMENT
(5) THE SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS

Respondents

IN THE INVESTIGATORY POWERS TRIBUNAL — Case No. IPT/13/204/CH
BETWEEN:

BYTES FOR ALL

Claimant

and

(1) THE SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS
(2) THE SECRETARY OF STATE FOR THE HOME DEPARTMENT
(3) THE SECRET INTELLIGENCE SERVICE
(4) THE SECURITY SERVICE
(5) THE GOVERNMENT COMMUNICATIONS HEADQUARTERS
(6) THE ATTORNEY GENERAL

Respondents

WITNESS STATEMENT OF CHARLES BLANDFORD FARR ON BEHALF OF THE RESPONDENTS

I, Charles Blandford Farr, of the Home Office, 2 Marsham Street, SW1P 4DF will say as follows:

1. I am Director General of the Office for Security and Counter Terrorism (OSCT) at the Home Office. I have held this position since June 2007. As Director General of OSCT, I am the senior official responsible for the UK counter terrorist strategy, CONTEST, and work on organised crime. I joined the Diplomatic Service in 1985 and have served at British Embassies in South Africa and Jordan. Since 2003, I have held a number of senior posts across Whitehall concerned with Security and Counter Terrorism.

2. I make this statement on behalf of the Respondents (by which I mean all Respondents in the five joined Claims).

3. Save where otherwise stated, all facts and matters referred to in this statement are true and within my own knowledge or have come to my attention during the course of my work. Insofar as facts and matters are not directly within my knowledge they are true to the best of my knowledge and belief.

4. Attached to this statement, and marked Exhibit 'CF1', are two bundles of relevant documents ('B1' and 'B2'). Tab and page numbers below are references to that Exhibit.

5. This statement addresses certain factual matters that are relevant to the preliminary issues of law identified by the Tribunal following the directions hearing on 14 February 2014, insofar as that can be done in "open" form.

6. In this statement I use the term "the Intelligence Services" to refer, collectively, to the Security Service, the Secret Intelligence Service and the Government Communications Headquarters. I also use the terms "SIS" and "GCHQ" to refer to the latter two bodies.

7. In this statement I will address, in turn, the following topics:

   (i) the relevant intelligence background for the preliminary issues of law;

   (ii) the factual background to the claims (insofar as that can be dealt with in an open witness statement);

   (iii) the relevant safeguards and oversight mechanisms; and

   (iv) various additional issues regarding interception under the Regulation of Investigatory Powers Act 2000 ("RIPA").

I. THE INTELLIGENCE BACKGROUND

8. The governments of democratic states are charged with the duty of upholding the criminal law and protecting their citizens from threats such as organised crime and terrorism. The UK has for many years faced a serious threat from terrorism. The threat in the UK from international terrorism in particular is currently assessed by the Joint Terrorism Analysis Centre ("JTAC") to be "Substantial", which means that an attack is assessed to be a strong possibility.

9. In a public speech given on 8 October 2013 (B1 tab 1 at page 3), the Director General of the Security Service (Andrew Parker) offered a fuller statement of the threat:

> "19. Turning to international terrorism, let's start with the plain facts: from 11 September 2001 to the end of March this year 330 people were convicted of terrorism-related offences in Britain. At the end of that period 121 were in prison, nearly three-quarters of whom were British. In the first few months of this year there were four major trials related to terrorist plots. These included plans for a 7/7-style attack with rucksack bombs, two plots to kill soldiers, and a failed attempt to attack an EDL march using an array of lethal weapons. There were guilty pleas in each case. 24 terrorists were convicted and sentenced to more than 260 years in jail.
> 20. Today, the threat level for international terrorism in the UK is assessed to be 'substantial': attacks are considered a strong possibility. But what does that really mean?
> 21. Since 2000, we have seen serious attempts at major acts of terrorism in this country typically once or twice a year. That feels to me, for the moment, unlikely to change.
> 22. While that tempo seems reasonably even, the ground we have to cover has increased as the threat has become more diversified."

10. The principal terrorist threat to the UK continues to derive from militant Islamist terrorists. As explained in the recent 2013 Annual Report by the Home Office on the UK's Counter-Terrorism Strategy, which is known as "CONTEST" ("the CONTEST Report" (B1 tab 2 at page 14):

> "1.6 The most significant development in connection with global terrorism during 2013 has been the growing threat from terrorist groups in Syria, where several factions of Al Qa'ida are active. Terrorist groups fighting in Syria have been supported by rapidly increasing numbers of foreign fighters, including numbers in the low hundreds from this country (many more than travelled to Iraq) and thousands from elsewhere. Dealing with terrorism in Syria is a very significant challenge due to the numbers of people fighting with the many Syria based terrorist groups, their proximity to the UK, ease of travel across porous borders and the ready availability of weapons. We are concerned about the threat to the UK from Syria based groups and the threat from foreign fighters returning to this country.

1.7 Although depleted, the Al Qa'ida senior leadership in the border areas of Pakistan and Afghanistan continues to call for global jihad, supports other local terrorist networks and has provided terrorist training for British nationals. Al Qa'ida affiliates have continued to pose a significant threat to the UK and UK interests, notably in Yemen, North and West Africa (where an Al Qa'ida splinter group conducted a significant attack against a gas facility in Algeria) and in Somalia. In Iraq terrorist attacks linked to Al Qa'ida have increased sharply, leading to over nine thousand fatalities in 2013. Across North Africa a growing number of smaller terrorist groups have emerged to pose an increasing threat to UK interests.
1.8 The terrorist threat to the UK comes from an increasingly wide range of countries and groups, many of which are new...."

11. The nature of the terrorist threat has also been affected by technological developments. In his open evidence to the Intelligence and Security Committee of Parliament ("the ISC"; for which see paragraphs 62-71 below) on 7 November 2013, the Director of GCHQ (Sir Iain Lobban) stated, in response to questions about the impact of technological change:

"On your question about terrorism, I think [technological change] has helped the terrorists. I think our job is harder, has got harder, is getting harder. If you think about what the internet does for terrorists, it gives them a myriad of ways to communicate covertly. It gives them a platform, to fund-raise, to radicalise, to spread propaganda. It gives them the means to plan, to command and control, to spread lethal ideas, to exhort violence." (See B1 tab 3 at page 29; the evidence of the three Heads of the Intelligence services begins at page 26).

12. There remains, also, a threat from Northern Ireland-related terrorism. The threat in Northern Ireland is assessed by JTAC to be "Severe", meaning that a terrorist attack is assessed to be highly likely. (The threat from Northern-Ireland related terrorism to Great Britain is assessed to be "Moderate", meaning a terrorist attack is possible but unlikely.)

13. The Government also regards serious and organised crime as one of the most significant threats to the UK. The National Crime Agency published a strategic assessment of serious and organised crime on 1 May 2014, which is at B1 tab 4 page 50.

14. In the face of this significant and enduring threat from terrorism, serious and organised crime and other national security threats there is a pressing need for the Intelligence Services and law enforcement agencies to be able to secure valuable intelligence in order to pursue their statutory objectives.

The sharing of intelligence with foreign states

15. Serious and organised criminals, terrorists and others who may seek to harm UK national security frequently operate and co-operate across national borders. Further, such individuals frequently seek to plan, prepare for, coordinate or carry out activities that may or that are designed to harm UK interests whilst they are outside the UK, or in association with others who are outside the UK.

16. As regards the threat from international terrorism, the CONTEST Report noted in this regard at paragraph 1.3 (B1 tab 2 page 14) that:

> "Although some terrorist plots here are developed entirely by British nationals living in this country, many of the threats we face continue to have significant overseas connections."

17. The activities of Al-Qaeda and its affiliates provide a particularly striking example of a type of terrorism that strives to operate on a global scale. Indeed, as the ISC notes in paragraph 6 of its most recent Annual Report (for 2012-2013), the number of terrorist groups outside the UK that have to be investigated is increasing as Al-Qaeda becomes more fragmented (B1 tab 5 page 84).

18. Technological change has also had an impact in relation to this issue. Sir Iain explained in his open evidence on 7 November 2013:

> "In terms of what [technological change] means for [GCHQ's] business, it means that we have to anticipate, discover, analyse, investigate and respond, and we have to do so globally because the threat is coming at us globally. We need a global, agile, flexible array of intelligence and security capabilities, and therefore we need global partnerships." (B1 tab 3 page 29).

19. Further, as regards serious and organised crime, the National Crime Agency's recent strategic assessment stated:

> "All of the most serious crime threats are transnational. Commodities of all types—including, for example, trafficked people destined for modern slavery, intangibles targeted in fraud and cyber crime—either come from or transit through often unstable countries." (B1 tab 4 page 54)

20. Given this background, it is highly unlikely that any government will be able to obtain all the intelligence it needs through its own activities. It is therefore vital for the UK Government to be able to obtain intelligence from foreign governments both to improve its understanding of the threats that the UK faces, and to gain the knowledge needed to counter those threats. Indeed, the intelligence that foreign governments share with the Intelligence Services (on a strictly confidential basis) represents a significant proportion of the Intelligence Services' total store of intelligence on serious and organised criminals, terrorists and others who may seek to harm UK national security. This store of intelligence forms a critical resource for the Government in seeking to take preventative action to counter threats, and save lives.

21. Intelligence from foreign governments is combined with intelligence obtained through the activities of the Intelligence Services to create a more complete picture of the threats to the UK, and to allow more effective identification of how these threats might be countered. These threats will frequently be common to more than one country and will most effectively be tackled by action taken by more than one government. It is therefore of great benefit to the UK Government for foreign governments also to have the fullest picture of the threats. For this reason it is highly desirable, where appropriate, for the Intelligence Services to be able to share intelligence that they have themselves acquired with foreign governments.

22. In its 2012-2013 Annual Report, the ISC noted at paragraph 7 the increasing importance for the Intelligence Services of collaborative working with partners overseas (B1 tab 4 page 84).

23. The Intelligence Services have particularly close and particularly productive ties with their intelligence counterparts in the US. These relationships are the result of over sixty years of successful collaboration, and proven trust. The immense value of these relationships for the UK in part reflects the fact that the US intelligence agencies are far larger and much better resourced than the Intelligence Services. (By way of illustration, it may be noted that the US intelligence budget in the 2012 fiscal year was $53.9 billion - see B1 tab 6 page 134 - which equates to approximately £34.5 billion, whilst the budget for the Intelligence Services in 2013-2014 was £1.9 billion.) In simple

terms, the US can provide the UK with intelligence that the UK - with its far more limited resources - could not realistically obtain by itself.

24. As regards interception in particular, and as the Interception of Communications Commissioner ("the Commissioner") noted at paragraph 6.8.6 of his 2013 Annual Report (B2 tab 14 page 914):

> "...information lawfully obtained by interception abroad is not necessarily available by interception to an interception agency here. In many cases it will not be available."

25. The Signals Intelligence ("Sigint") relationship between the UK and the US was codified in 1946 by what is often referred to as "the UKUSA agreement". (Signals Intelligence covers intelligence produced from intercepting communications, but also from other electronic signals, such as radar transmissions.) The UKUSA agreement has been in the public domain since 2010, when it was released by GCHQ to the National Archives (see B1 tab 7 page 135). The agreement provides for the exchange of "foreign communications" information (as defined at page 140) and operational methods between the US and UK. The agreement recognises there will be circumstances in which either party may choose not to share categories of information, and it stipulates that information derived from communications intelligence sources may not be exploited for commercial purposes, but it otherwise anticipates an extensive degree of sharing (based on the presumption of shared values and aligned national interests). The Sigint agencies of Canada, Australia and New Zealand became parties to the agreement by virtue of arrangements put in place in appendices to the agreement (see Appendix J of HW 80/6 and Annexure J1 to Appendix J of HW 80/11, at pages 222 and 224 respectively). The material in the National Archives also makes clear that any of the five parties to the expanded arrangement may request assistance from any other (see paragraph 8 of the Introduction to the Appendices of HW 80/6, at page 147) and that the five parties effect a division of effort on interception tasks between them (see page paragraph 9 of the Introduction to the Appendices of HW 80/6, at page 147). Any sharing of intelligence by the UK Intelligence Services pursuant to the UKUSA agreement must, of course, comply fully with UK law.

26. Overall, intelligence derived from communications and communications data obtained from foreign intelligence partners, and from the US intelligence agencies in particular,

has led directly to the prevention of terrorist attacks and serious crime, and the saving of lives.

The sharing of intelligence deriving from interception as compared with other forms of intelligence

27. Paragraphs 15-22 above do not just apply to intelligence obtained through interception. These paragraphs apply to all forms of intelligence, including intelligence (i) derived from covert human intelligence sources (as they would be termed under RIPA), (ii) derived from or constituting records of audio and/or visual surveillance and (iii) obtained or derived from covert property searches.

28. I am advised that a potential issue in these proceedings is whether the sharing of intelligence in the form of (or that is derived from) communications and communications data between the UK and foreign governments should in some sense be separately regulated.

29. From the point of view of the privacy interests of those individuals who are subject to investigative measures, I do not consider that a workable distinction can be drawn between such intelligence and the other three forms of intelligence referred to in paragraph 27 above. In particular, I do not consider that intelligence in the form of (or that is derived from) communications and communications data is in some general sense more personal or private than those other forms of intelligence. For instance, if an eavesdropping device is covertly installed in a target's home it may record conversations between family members that are more intimate and personal than those that might be recorded if the target's telephone were to be intercepted (and this example becomes even clearer if, for instance, the telephone in question is only used by the target to contact his criminal associates). To give a further example, a covert human intelligence source may be able to provide information about a target as a result of his or her friendship (or more intimate relationship) with the target that is more private than information that could be obtained from, for instance, intercepting the target's emails.

30. Nor can some general distinction be drawn between intelligence from interception and the other forms of covert intelligence identified in paragraph 27 above in terms of how

likely it is that the individual targets in question will in practice be able to predict or foresee the possibility of the relevant investigative measures being taken against them. All forms of covert intelligence-gathering necessarily seek to benefit from a lack of awareness on the part of the target in order to maximise the chance of obtaining valuable intelligence. Interception is, in this regard, no different from, for instance, covert surveillance or the use of covert human intelligence sources.

The importance and value of interception under RIPA

31. Interception under RIPA provides tactical information for the Intelligence Services and law enforcement agencies. When yielding tactical information, RIPA interception provides real time intelligence on the plans and actions of individual terrorists, criminals and other targets, which allows the Intelligence Services to disrupt or frustrate their plans. Such information also enables evidence against targets to be obtained, and facilitates their arrest by law enforcement agencies. Other information that is obtained via interception is used to identify other previously unknown communications of existing targets, and to identify new targets for investigation. Indeed, a significant proportion of initial intelligence leads derive from interception operations. Information obtained from interception is also used to investigate and assess the potential importance, plans, international connections and operating methods of existing targets, from which (along with intelligence from other sources) a broad understanding of the terrorist and criminal threat facing the UK can be derived, and preventive strategies developed.

32. I have read a number of documents which detail the value and importance of intelligence which has been gathered under RIPA. It is not possible to disclose the documents themselves because they contain highly classified information. I can, however, confirm that such intelligence has led directly to the prevention of terrorist attacks and serious crime, the success of operations aimed at countering the proliferation of weapons of mass destruction and the saving of lives. Overall, RIPA interception is a critical tool in investigations into the full range of threats to national security.

33. The Commissioner has consistently confirmed the value and importance of the interception powers under RIPA. For instance, the Commissioner stated in his 2011 Annual Report, at paragraph 5 (B2 tab 12 page 718):

> "Interception remains a powerful technique in the investigation of many types of crime and threats to national security. Many of the largest drug-trafficking, fiscal evasion, people-trafficking, counter-terrorism and wider national security and serious crime investigative successes of the recent past have in some way involved the use of interception and communications data."

34. The Commissioner again confirmed the value of interception in the Foreword to his 2012 Annual Report (see B2 tab 13 page 781):

> "Lawful interception and communications data acquisition remain crucial techniques for the UK's intelligence agencies, law enforcement bodies and wider public authorities to use in pursuit of their statutory objectives."

II. THE FACTUAL BACKGROUND TO THE CLAIMS

The US "Prism" programme and US "upstream collection"

35. Insofar as the intelligence activities and operations of the US Government have been the subject of official statements and/or other express avowal by the executive branch of the US Government, I accept the truth of those official statements and/or avowals, and do not seek to adopt a neither confirm nor deny stance in relation to them. (For the avoidance of doubt, and for the reasons set out in paragraph 46 below, I adopt the usual neither confirm nor deny stance in relation to any information on the intelligence activities and operations of the US Government that is derived from any alleged leak insofar as that information has not been positively confirmed by an official statement by the executive branch of the US Government, or otherwise avowed by it.)

36. I therefore accept, in this "open" witness statement, the existence of the US "Prism" programme, as it has been expressly avowed by the executive branch of the US Government. In particular, in a statement dated 8 June 2013 (B1 tab 8 page 228), Mr James Clapper, who is the US Director of National Intelligence, confirmed Prism to be an internal US Government computer system used to facilitate the US Government's

collection of foreign intelligence information from electronic communication service providers under US Court supervision, as authorised by s. 702 of the Foreign Intelligence Surveillance Act 1978 ("FISA").

37. I similarly accept the existence of the US "upstream collection" programme, as this has been expressly avowed by the executive branch of the US through its declassification of parts of a US FISA Court judgment (see B1 tab 9 page 231 and in particular page 232). As appears from this judgment extract, the upstream collection programme operates under s. 702 of FISA and involves internet communications being obtained (subject to US Court supervision) as they transit the internet.

38. More generally, the National Security Agency's document of 9 August 2013, "*The National Security Agency: Missions, Authorities, Oversight and Partnerships*" (B1 tab 10 page 242) confirms the following:

> "Under Section 702 of the FISA, NSA [i.e. the National Security Agency] is authorized to target non-U.S. persons who are reasonably believed to be located outside the United States. The principal application of this authority is in the collection of communications by foreign persons that utilize U.S. communications service providers. The United States telecommunications system and FISA is designed to allow the U.S. Government to acquire foreign intelligence while protecting the civil liberties and privacy of Americans. In general, Section 702 authorizes the Attorney General and Director of National Intelligence to make and submit to the FISA Court written certifications for the purpose of acquiring foreign intelligence information. Upon the issuance of an order by the FISA Court approving such a certification and the use of targeting and minimization procedures, the Attorney General and Director of National Intelligence may jointly authorize for up to one year the targeting of non-United States persons reasonably believed to be located overseas to acquire foreign intelligence information. The collection is acquired through compelled assistance from relevant electronic communications service providers.
>
> NSA provides specific identifiers (for example, e-mail addresses, telephone numbers) used by non-U.S. persons overseas who the government believes possess, communicate, or are likely to receive foreign intelligence information authorized for collection under an approved certification. Once approved, those identifiers are used to select communications for acquisition. Service providers are compelled to assist NSA in acquiring the communications associated with those identifiers.
>
> ....

The collection under FAA Section 702 is the most significant tool in the NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the U.S. and around the world ...." (Original emphasis.)

39. This NSA document further confirms that, in its foreign intelligence mission, the NSA "touches" approximately 1.6% of the data carried over the internet, and only selects 0.025% of that data for review (*i.e.* analysts only look at 0.00004% of the world's total internet traffic).

40. I note that the NSA has also recently published a report on its implementation of s. 702 of FISA, which makes further reference to the Prism programme and to upstream collection (see B1 Tab 11 and in particular page 252).

41. Further, in all the specific circumstances of the present case, including in particular in the light of the ISC's public Statement of 17 July 2013 which I address at paragraphs 72-74 below, I am able to confirm that GCHQ has obtained information from the US Government that the US Government obtained via Prism. However, beyond this confirmation, I maintain on the Respondents' behalf the ordinary "neither confirm nor deny" stance for intelligence matters (for which, see paragraphs 42-45 below). Accordingly, I do not set out in this open witness statement any further indication of the timing, nature or extent of GCHQ's access to information via Prism. Further, and for the avoidance of doubt, I (i) neither confirm nor deny that either the Security Service or the SIS has obtained, from the US Government, information that has been obtained under the Prism programme and (ii) neither confirm nor deny that any of the Intelligence Services has obtained, from the US Government, information that has been obtained under upstream collection.

The alleged Tempora operation

42. As has been explained at paragraphs 5-10 of the Open Response, secrecy is essential to the covert work and operational effectiveness of the Intelligence Services, whose primary function is to protect national security. If a terrorist was to become aware that they were the subject of interest by the Intelligence Services, they could take steps to thwart any investigation or operation. Conversely, if a terrorist was to become aware

that they were not the subject of Intelligence Service interest, they would then know that they could engage in their activities with increased vigour and confidence.

43. In addition, secrecy must be maintained in respect of the intelligence-gathering capabilities and techniques of the Intelligence Services (and any gaps in or limits to those capabilities and techniques). If hostile individuals or groups were to acquire detailed information on such matters then they would be able to adapt their conduct to avoid, or at least minimise, the risk that the Intelligence Services could successfully deploy those capabilities and techniques against them. It is particularly important that an appropriate degree of secrecy is maintained as regards the methods by which any interception may be effected. Failure to do so will inevitably and seriously reduce the effectiveness of interception techniques. The Government will therefore be less able to acquire the vital intelligence that it needs to protect its citizens. In particular, if possible targets of interception are able to gain insights into sensitive interception techniques and capabilities then they will use those insights to try to minimise the chance that any future use of interception powers will yield valuable intelligence against them. This is not simply a theoretical possibility: it is a real practical risk. Terrorists and sophisticated criminal gangs are known to take a keen interest in the capabilities and practices of the authorities that may be seeking to discover their plans. The Government has had experience of information about surveillance methods being put into the public domain, leading directly to the loss of important sources of intelligence.

44. Where the disclosure of information about targets, methods or capabilities would cause direct damage to national security interests, there is a clear and obvious need for secrecy, over and above any "neither confirm nor deny" considerations. But there will be many other circumstances where a disclosure by the Intelligence Services would not on first glance cause any such damage. Take, for example, the case where an individual alleges that he is being targeted by the Intelligence Services, when he is in fact of no interest to them. It might not cause any damage to national security in that particular case for the Intelligence Services to deny any targeting of that individual. However, such a denial has the real potential to cause indirect national security damage. This is because there may be a future case where a similar allegation is made by a person or organisation who is of genuine interest to the Intelligence Services. Damage would of course be caused by confirming the allegation, but damage would

also be caused by a "no comment" response as it would be interpreted as an inferred admission, given the previous denial.

45. To avoid this more indirect but nevertheless serious damage to national security, it has been the policy of successive UK Governments to neither confirm nor deny who they may or may not be monitoring, and with whom they may or may not have had contact. Similarly, the neither confirm nor deny principle has been applied to the truth of claims about the operational activities of the Intelligence Services, including in particular intelligence-gathering capabilities and techniques.

46. This approach is particularly important in the context of leaks and other unauthorised disclosures of sensitive information. The neither confirm nor deny principle would be fatally undermined, and national security thereby seriously damaged, if every time sensitive information was leaked, or it was alleged that there had been such a leak, the Government was then obliged to confirm or deny the veracity of the information in question. It has thus also been the policy of successive Governments to adopt a neither confirm nor deny stance in relation to any information derived from any alleged leak regarding the activities or operations of the Intelligence Services insofar as that information has not been separately confirmed by an official statement by the Government.

47. In this case, I understand it is argued that the Government should depart from its usual policy of neither confirm nor deny in relation to the alleged Tempora interception operation, on the basis that journalists have obtained "genuine" documents which refer to it, whose provenance (it is said) has been accepted by the Government. I do not consider that this allegation places the present case in any different category from that of any other alleged leak. The Government has accepted that Mr Miranda was in possession of approximately 58,000 stolen classified GCHQ documents when he was stopped pursuant to Schedule 7 of the Terrorism Act 2000 powers at Heathrow Airport on 18 August 2013. However, the Government has not accepted the provenance of the documents which formed the basis for the media articles on the alleged Tempora interception operation; nor has the Government confirmed or denied the provenance of any particular document that is alleged to have been stolen by Mr Snowden.

48. In accordance with the Government's usual policy of neither confirm nor deny, I can therefore make no admission as to the veracity or otherwise of Factual Premise (4) in the Tribunal's Directions. I am not aware of any exceptional circumstances which would justify a departure from the neither confirm nor deny principle in relation to the alleged Tempora interception operation. All I am able to confirm is that, if the Tempora interception operation existed, it would have been carried out under the authority of the section 8(4) regime as set out at §§ 102-178 of the Open Response.

III. SAFEGUARDS AND OVERSIGHT

The intelligence sharing and handling regime: safeguards

49. Paragraphs 36-76 of the Open Response set out the regime that governs the sharing of intelligence between the Intelligence Services and foreign governments, and the handling and use of foreign intelligence obtained as a result. The regime imposes specific statutory limits on the information that each of the Intelligence Services can obtain, and on the information that each can disclose. At B1 tab 12 pages 258 to 281 are copies of the Ministerial certificates (under section 28 of the Data Protection Act 1998) for the three Intelligence Services to which reference is made in paragraph 53 of the Original Open Response.

50. By virtue of section 19(2) of the Counter-Terrorism Act 2008, intelligence obtained by any of the Intelligence Services in connection with the exercise of any of its functions may in principle be used by that service in connection with the exercise of any of its other functions. This means, for example, that intelligence that is obtained by the Security Service for national security purposes can as appropriate be subsequently used by the Security Service to support the activities of the police in the prevention and detection of serious crime. This degree of operational flexibility regarding the use of intelligence is necessary not least because of the overlap in practice between the various statutory functions of the Intelligence Services, and the fact that a given item of intelligence may be of relevance to more than just the particular purpose for which it was first acquired.

51. The Intelligence Services take their legal duties under the regime very seriously. The statutory framework is underpinned by detailed internal guidance (including the

"arrangements" to which reference is made in section 2 of the Security Service Act 1989and sections 2 and 4 of the Intelligence Services Act 1994), and by a culture of compliance.

52. This culture of compliance is reinforced by the provision of mandatory training to staff within the Intelligence Services regarding the legal and policy framework within which they operate. The training includes clear instructions on the need for strict adherence to the law and to internal guidance.

53. Further, all staff who operate under the regime that governs the sharing of intelligence between the Intelligence Services and foreign governments (and the handling and use of foreign intelligence obtained as a result) are appropriately vetted to ensure that they will faithfully operate within the aims, safeguards and ethos of the Intelligence Services. The Government's policy on security vetting was announced to Parliament by the then Prime Minister in 1994. The policy is now set out in a Cabinet Office booklet, "*HMG Personnel Security Controls*", most recently reissued in April 2014 (B1 tab 13 page 282).(The same policy applies to all staff in the Intelligence Services who undertake interception operations.)

54. There are also procedures in place to ensure that if, despite all precautions being taken, the internal guidance is found not have been properly applied, staff are directed immediately to cease the activity in question, take any necessary remedial action they may be directed to undertake and report the matter to management. While an isolated failure to properly apply the guidance is not (normally) grounds for censure, not reporting to management is treated as a very serious matter.

The confidentiality of the arrangements governing intelligence sharing and handling

55. The full details of the arrangements between the Intelligence Services and the UK's foreign intelligence partners for the sharing of intelligence, and the internal guidance of the Intelligence Services for the handling and use of intelligence obtained as a result, are (and have always been) kept confidential. I am satisfied that they cannot safely be published without undermining the interests of national security and the prevention and detection of serious crime. There are four main reasons for this.

56. First, it is vital that the specifics of the intelligence sharing / handling arrangements are kept secret in order to avoid revealing existing intelligence-gathering capabilities and relationships, and gaps or shortcomings in those capabilities and relationships. If such secrecy is not maintained the effectiveness of the arrangements will inevitably and seriously be reduced, and the Government will be less able to acquire and make productive use of the vital intelligence that it needs to protect its citizens. In particular, hostile individuals would be able to (and would) use the information so disclosed to adapt their conduct in an effort to minimise the chance that any future use of the intelligence sharing / handling arrangements might yield valuable intelligence against them.

57. For example, an individual intent on undertaking terrorist training overseas may have the choice of undertaking that training in state A or state B. If the Government openly published the intelligence sharing relationships with the two states in issue, that individual could form a view as to the types of intelligence that the Government might pass to or receive from those states, and as to the circumstances in which such intelligence sharing might occur. In an effort to ensure that his terrorist training remained undetected for as long as possible, the individual would likely choose to undertake terrorist training in the state which shared the least amount of potentially relevant intelligence with the UK. This would of course in turn make it harder for the Intelligence Services to detect the individual's activities and disrupt any threat that he might pose to national security.

58. Secondly, publishing further details of the intelligence sharing arrangements may pose acute difficulties for the liaison relationships between the Intelligence Services and their foreign intelligence partners. Some foreign states choose to have intelligence sharing relationships with the UK on the strict understanding that the existence of those relationships will be kept confidential. If the Government were obliged to publish details of such relationships it is possible that those states would discontinue them, leading to a significant reduction in the intelligence available to the Intelligence Services. Similarly, some states may be content to avow publicly their intelligence sharing relationship with the UK, but may not want to describe publicly all the types of intelligence that are shared as a result (to avoid disclosing the full range of their

intelligence-gathering capabilities). If further details of the intelligence sharing arrangements were published such states might choose to restrict the intelligence they shared with the UK to those types of intelligence that they were prepared to publicly admit that they acquire or collect. This would similarly reduce the quality and quantity of intelligence available to the Intelligence Services.

59. Thirdly, it is necessary to avoid being too specific in any published materials regarding the intelligence sharing / handling arrangements in order not to limit operational flexibility in the light of changing circumstances (including the developing nature of the threats posed to UK national security) and technological developments. For example, as regards the latter, certain technological advances may offer those in relation to whom intelligence is required for the protection of the public (for instance, terrorists) greater opportunities to evade intelligence gathering techniques, with a consequent need for the Intelligence Services to adapt their intelligence-gathering methods. As the Commissioner noted as far back as 2001 (see paragraph 45 of his 2000 Annual Report, at B2 tab 1 page 440):

> "The task of the Agencies working in this field has become much more difficult and complex as a result of the proliferation of mobile telephones and the greater sophistication of criminals and terrorists."

60. There are also practical impediments to putting more detailed information into the public domain. The pace of technological development, combined with other changes in circumstances including the changing threat from different parts of the world, is such that the published detailed provisions would quickly become outdated, and hence either unduly restrictive or insufficiently effective, and would thus need to be revised. Further, and significantly, the nature and scope of any necessary revisions would themselves offer additional insights into the activities of the Intelligence Services (and changes in their methods and priorities) which would further assist terrorists and others hostile to UK interests to avoid or minimise the risk that any future use of the intelligence sharing / handling arrangements might yield valuable intelligence against them. This is the fourth reason why the specific details of those arrangements need to be kept secret.

61. The above difficulties would apply even if the Government were only required to publish more information in relation to the sharing of intercepted communications and communications data with foreign intelligence partners and the subsequent handling and use of such communications and communications data. However, if – as I have sought to suggest in paragraphs 27-30 above – no workable distinction can in fact be drawn on privacy or foreseeability grounds between these forms of intelligence and other forms of intelligence, and the Government were required to publish more information on the sharing / handling of all intelligence, the above three difficulties would only become more acute.

Parliamentary oversight: the role of the Intelligence and Security Committee of Parliament

62. SIS and GCHQ are responsible to the Foreign Secretary. The Security Service is responsible to the Home Secretary. Those Secretaries of State are in turn of course accountable to Parliament.

63. In addition, the ISC also plays an important part in overseeing the intelligence-gathering activities of the Intelligence Services. In particular, the ISC is the principal method by which scrutiny by Parliamentarians is brought to bear on those activities.

64. The ISC, in its original form, was established by the Intelligence Services Act 1994. On 25 June 2013, the ISC was reconstituted under the Justice and Security Act 2013 ("the JSA"). From that date onwards, the JSA has provided the governing statutory framework for the ISC. In its Annual Report for 2012-2013 (B1 tab 5), the ISC stated that it welcomed the changes in the JSA and that those changes were "broadly in line with those we ourselves had previously recommended to the Government, and which will increase accountability" (at page 83).

65. The ISC is an all-party body of nine Parliamentarians drawn from both the House of Commons and the House of Lords, each member being nominated for membership by the Prime Minister in consultation with the leader of the opposition, and appointed by the House of Parliament from which they are drawn. The Government has no power to remove a member of the ISC. The current chair of the ISC is The Rt Hon Sir Malcolm

Rifkind QC MP, who was the Secretary of State for Defence (1992-1995) and the Foreign Secretary (1995-1997). Under the JSA, any future Chair will be appointed by the Committee from amongst its members, rather than being appointed by the Prime Minister, as was formerly the case (and was the case for Sir Malcolm).

66. The ISC operates within the "ring of secrecy" which is protected by the Official Secrets Act 1989. It may therefore consider classified information, and in practice takes oral evidence in closed session from the Foreign and Home Secretaries, the three Heads of the Intelligence Services, and their staff. (The ISC also may hold open evidence sessions. The ISC held its first ever open evidence session on 7 November 2013, to which I have referred at paragraph 11 and 18 above, at which evidence was given by the three Heads of the Intelligence Services.)

67. The ISC meets at least weekly whilst Parliament is sitting. It is supported by staff who have the highest level of security clearance. The Heads of the Intelligence Services are under a general obligation to arrange for any information requested by the ISC in the exercise of its functions to be made available to it. The power to refuse such a request has been removed from the Heads of the Intelligence Services and now lies with Ministers alone, who can only exercise this power in certain limited circumstances.

68. The ISC's statutory role is to examine or otherwise oversee the expenditure, administration, policy and operations of the Intelligence Services. The ISC will also in due course be able to examine or otherwise oversee such other activities of Government in relation to intelligence or security matters as are set out in a memorandum of understanding. The details of the memorandum in question are currently close to finalisation. The ISC will publish the memorandum of understanding when it is agreed, and will lay a copy of it before Parliament. (The ISC has already started to use its new powers to oversee operational matters. In particular, the ISC was asked by the Prime Minister to use its new powers to investigate, among other things, what was known - prior to the May 2013 attack on Drummer Lee Rigby in Woolwich - about the perpetrators, whether any more could have been done to stop them and the lessons to be learnt. In investigating these matters the ISC has seen underlying documents from all the Intelligence Services and has also questioned the Heads of the Intelligence Services and senior staff at length.)

69. In order to be able effectively to carry out its expanded remit under the JSA, the ISC's budget has been substantially increased and the ISC is in the process of recruiting further staff. This will result in a three-fold increase in the ISC's investigative capacity.

70. The ISC sets its own agenda and work programme. It is required to make an annual report to Parliament on the discharge of its functions. It may issue reports more frequently and has previously done so for the purposes of addressing specific issues relating to the work of the Intelligence Services that it has chosen to investigate or otherwise consider. Where necessary, the ISC's reports are redacted to ensure that they do not contain any sensitive information that would be prejudicial to the continued discharge of the functions of any organisation, or part of an organisation, for which the ISC has an oversight responsibility (albeit that the ISC may report any redacted matters to the Prime Minister). The ISC also monitors the Government to ensure that any recommendations it makes in its reports are acted upon. In addition, the Government lays before Parliament any response that it makes to the ISC's reports.

71. The ISC's reports illustrate its proactive approach to oversight and reveal the thoroughness with which it scrutinises the Intelligence Services. The level of detail in the information and evidence that the Government provides to the ISC is clear both from the ISC's annual reports and its reports on individual topics. In particular, the reports demonstrate that, where it is necessary to do so for the purposes of overseeing the full range of the activities of the Intelligence Services, the ISC is provided with all such sensitive information as it needs. The ISC's Annual Report for 2012-2013 (at B1 tab 5) and its Report on Foreign Involvement in the Critical National Infrastructure (at B1 tab 14) illustrate these points (see, for instance the Annual Report at page 83). For completeness, and to illustrate how seriously the ISC's reports are taken by Government, Exhibit CF1 also contains the Government's formal response to these two reports (B1 tab 15 at pages 338 and 344A).

The ISC's investigations in the light of media reports on Prism and related matters

72. In the light of reports in the media on Prism in the summer of 2013, the ISC decided to investigate an allegation made in some of those reports to the effect that GCHQ had

acted illegally by accessing communications content via the Prism programme. In particular, it was asserted that GCHQ had had access to Prism and thereby to the content of communications in the UK without proper authorisation and it was further asserted that, by so doing, GCHQ had circumvented UK law. The ISC published a Statement on its investigation on 17 July 2013 (B1 tab 16 page 345). In paragraph 5 of that Statement the ISC set out how it had conducted its investigation:

> "The ISC has taken detailed evidence from GCHQ. Our investigation has included scrutiny of GCHQ's access to the content of communications, the legal framework which governs that access, and the arrangements GCHQ has with its overseas counterparts for sharing such information. We have received substantive reports from GCHQ, including:
> - a list of counter-terrorist operations for which GCHQ was able to obtain intelligence from the US in any relevant area;
> - a list of all the individuals who were subject to monitoring via such arrangements who were either believed to be in the UK or were identified as UK nationals;
> - a list of every 'selector' (such as an email address) for these individuals on which the intelligence was requested;
> - a list of the warrants and internal authorisations that were in place for each of these individual being targeted;
> - a number (as selected by us) of the intelligence reports that were produced as a result of this activity; and
> - the formal agreements that regulated access to this material.
>
> We discussed the programme with the NSA and our Congressional counterparts during our recent visit to the United States. We have also taken oral evidence from the Director of GCHQ and questioned him in detail."

73. In the light of its investigation, the ISC's conclusions were as follows:

> "• It has been alleged that GCHQ circumvented UK law by using the NSA's PRISM programme to access the content of private communications. From the evidence we have seen, we have concluded that this is unfounded.
> - We have reviewed the reports that GCHQ produced on the basis of intelligence sought from the US, and we are satisfied that they conformed with GCHQ's statutory duties. The legal authority for this is contained in the Intelligence Services Act 1994.
> - Further, in each case where GCHQ sought information from the US, a warrant for interception, signed by a Minister, was already in place, in accordance with the legal safeguards contained in [RIPA]."

74. The ISC noted that GCHQ had "rightly" put in place policies and procedures that were more detailed than some of the governing legislative provisions (paragraph 8 of the Statement of 17 July 2013). Further, and although it found (see paragraph 6 of the

Statement) that GCHQ had not circumvented or attempted to circumvent UK law, the ISC concluded that it would nevertheless be proper to "... consider further whether the current statutory framework governing access to private communications remains adequate."

75. On 17 October 2013, the ISC announced that it would be broadening this review of the legislative framework governing the Intelligence Services' access to the content of private communications to consider, additionally, the appropriate balance between privacy and security in an internet age (B1 tab 17 page 348). Sir Malcolm Rifkind said:

> "In recent months concern has been expressed at the suggested extent of the capabilities available to the intelligence agencies and the impact upon people's privacy as the agencies seek to find the needles in the haystacks that might be crucial to safeguarding national security. There is a balance to be found between our individual right to privacy and our collective right to security. An informed and responsible debate is needed. The [ISC] has therefore decided to broaden the scope of its forthcoming inquiry to consider these wider questions, in addition to those relating to the existing legislative framework."

76. On 11 December 2013, and as part of this broader review, the ISC issued a "Call for Evidence" from members of the public and organisations outside Government (B1 tab 18 page 350). Further, and as noted in that Call for Evidence, the ISC intends to hold oral evidence sessions once it has finished reviewing the written submissions received as a result.

The role of the Secretaries of State in issuing and renewing section 8(4) warrants

77. Section 5 of RIPA provides that, in general, a warrant, including a warrant that complies with section 8(4), has to be personally issued by the Secretary of State, on an application to him to that effect. Further, under section 8(6) of RIPA, the certificate for a section 8(4) warrant can only be issued by the Secretary of State. The purposes for which warrants may be issued are set out in section 5(4) of RIPA. As the Commissioner noted in paragraph 3.8 of his 2013 Report, "Secretaries of State do not issue interception warrants for other purposes" (B2 tab 14 at page 858).

78. Applications for section 8(4) warrants must contain all the detailed matters set out in paragraph 5.2 of the current Interception of Communications Code of Practice ("the

Code"; as regards applications for renewals, paragraph 5.12 of the Code also applies). In his 2013 Report, the Commissioner stated at paragraph 3.39:

> "My inspections demonstrate that the paperwork is almost always compliant and of a high quality. If there are occasional technical lapses, these are almost always ironed out in the interception agencies themselves or in the Secretary of State's department before the application reaches the relevant Secretary of State." (Page 863).

79. Further, the Commissioner has consistently taken the view that the Secretaries of State provide, in effect, a real and practical safeguard. In paragraph 3.40 of his 2013 Annual Report, the Commissioner commented:

> "The Secretaries of State themselves are entirely conscientious in undertaking their RIPA 2000 Part I Chapter I duties. They do not rubber stamp applications. On the contrary, they sometimes reject applications or require more information." (Page 863).

80. To similar effect, the Commissioner noted at paragraph 3.10 of the 2013 Annual Report that warrants are on occasions "refused ... where it is judged that the necessity does not outweigh the intrusion" (page 858). Further, as regards section 8(4) warrants in particular, the Commissioner found as follows in paragraph 6.5.43 of his 2013 Annual Report:

> "• the Secretaries of State who sign warrants and give certificates are well familiar with the process; well able to judge by means of the written applications whether to grant or refuse the necessary permissions; and well supported by experienced senior officials who are independent from the interception agencies making the applications;
> • if a warrant is up for renewal, the Secretary of State is informed in writing of the intelligence use the interception warrant has produced in the preceding period. Certificates are regularly reviewed and subject to modification by the Secretary of State ...."

81. The Foreword of the Commissioner's 2012 Annual Report similarly recognised that the Secretaries of State take their responsibilities "very seriously" (B2 tab 13 at page 781), and further statements to this effect may be found in paragraph 6.6.1 and 6.6.2 of that Report (page 799).

82. I respectfully agree with and endorse the above statements by the Commissioner.

Oversight by the Interception of Communications Commissioner

83. Bundle 2 of Exhibit CF1 contains the Annual Reports of the Commissioner for the years 2000 to 2013 (the year of the most recent report). As from 1 January 2013, the Interception of Communications Commissioner ("the Commissioner") has been Sir Anthony May, the former Lord Justice of Appeal. His predecessor was Sir Paul Kennedy (also a former Lord Justice of Appeal).

84. In paragraphs 6.3.1-6.3.4 of the 2013 Annual Report, the Commissioner emphasised his independence from government and from the intercepting agencies, including the Intelligence Services (B2 tab 14 pages 895-896). He further noted that his investigations are "thorough and penetrating" and that he has "no hesitation in challenging the public authorities wherever this has been necessary" (see paragraph 6.3.3).

85. By section 58(1) of RIPA a duty is imposed on, among other persons, every person holding office under the Crown to disclose and provide to the Commissioner all such documents and information as he may require for the purpose of enabling him to carry out his functions. As the Commissioner noted in paragraph 2.14 of his 2013 Annual Report:

> "I have found that everyone does this without inhibition. I am thus fully informed, or able to make myself fully informed, about all the interception and communications data activities to which RIPA 2000 Part I relates however sensitive these may be." (Page 856)

86. Similarly, Section 6 of the 2013 Annual Report – which sets out and answers various "Questions of Concern" - contains the following (page 893):

> **"1. Does the Interception of Communications Commissioner have full access to all information from the public authorities sufficient for him to be able to undertake his statutory functions?**
>
> **6.1.1** Yes. All those engaged in RIPA 2000 Part I matters have a statutory obligation to disclose and provide to me all such documents and information as I may require for the purpose of enabling me to carry out my statutory functions (section 58(1) ...).

6.1.2 This means that I have unrestricted access to full information, however sensitive, about the activities I am required to review. I can report that I am in practice given such unrestricted access and that all of my requests (of which there have been many) for information and access to material or systems are responded to in full. I have encountered no difficulty from any public authority or person in finding out anything that I consider to be needed to enable me to perform my statutory functions. On the contrary, the public authorities are keen that I should fully understand what I consider I need to know. They frequently volunteer information which they consider I ought to know or which they think would be useful."

87. In the discharge of his functions the Commissioner inspects all the agencies (including all the Intelligence Services) that are authorised to apply for interception warrants, and the work of senior officials and staff in the relevant parts of the main Departments of State. During 2013, the Commissioner visited each agency twice (see paragraph 3.30 of the 2013 Annual Report, at page 861 B2). This is in keeping with the practice of the previous Commissioner (Sir Paul Kennedy), as is clear from paragraph 6.2 of the 2012 Annual Report (page 790 B2).

88. The current Commissioner has also inspected the work of the senior officials and staff in the relevant parts of the main Departments of State at six monthly intervals (paragraph 3.33 of the 2013 Annual Report, at page 862 B2).

89. As regards the second set of inspections of the agencies in 2013, the Commissioner commented as follows at paragraph 3.32 of his 2013 Annual Report (at page 862 B2):

"• we increased the inspection time spent with each interception agency. Most of the inspections ran over two days, the first of which we generally used for reading warrantry and other documents in preparation for the second day's investigations. These investigations covered those selected operations or warrants which required further explanation;
- we carried out or continued a full investigation where necessary into matters raised by media disclosures;
- we instigated a thorough investigation of the arrangements in place for the Retention, Storage and Destruction of intercepted material and related communications data ....;
- we instituted what will now become our standard procedure of producing a detailed written report and recommendations from each inspection. This is sent to the Head of the relevant interception agency with a copy for the relevant Secretary of State."

(I address the second bullet point in more detail at paragraphs 110-125 below, and the third bullet point in more detail at paragraphs 105-106 below.)

90. Paragraph 3.35 of the 2013 Annual Report addresses the inspection of warrants, as referred to in the first of the above bullet points:

> "We inspect the systems in place for applying for and issuing interception warrants under sections 8(1) and 8(4). We scrutinise what I regard as a representative sample (chosen by me) of the warrantry paperwork. In this context warrantry paperwork includes warrant applications, renewals, modifications, cancellations and their associated instruments and schedules. Much of this is on paper, but in some interception agencies we now have access to and personally interrogate the computer systems that the agencies use. This enables us to audit the process from start to end and to examine the product gained from the interception." (Page 862 B2.)

91. I can further confirm, from having examined the relevant records, that section 8(4) warrants were regularly amongst those examined by the previous Commissioner.

92. Since 1 July 2002, the Commissioner has, when examining warrants, checked to ensure that the guidance in the Code has been complied with. This remains the position under the current Commissioner (see paragraph 3.29 of the 2013 Annual Report, at page 861 B2).

93. The fourth bullet point in paragraph 3.32 of the 2013 Report (set out in paragraph 86 above) refers to the Commissioner's inspection reports, which are more fully addressed in paragraph 3.38 of the 2013 Annual Report:

> "The reports contain formal recommendations with a requirement for the interception agency to report back to me within two months to say that the recommendations have been implemented, or what progress has been made. These are sensitive documents, but, speaking generally, they contain:
> - an account of the inspection, including a list of the particular warrants inspected;
> - assessments of the interception agency's compliance with statutory requirements;
> - an account of the errors reported by the interception agency to my office during the inspection period; and
> - a number of structural recommendations aimed at improving the interception agency's compliance and performance generally." (Page 863 B2.)

94. On average, the Commissioner made approximately 7 recommendations for each agency (paragraph 3.41 of the 2013 Annual Report, at page 863 B2). He proposes to check on progress in implementing those recommendations during 2014 (paragraph 3.47 of the 2013 Annual Report, at page 865 B2).

95. The Commissioner also visited the main warrant issuing Secretaries of State at the end of 2013 or early in 2014 (paragraph 3.33 of the 2013 Annual Report). Again, this is in keeping with the practice of the previous Commissioner (see paragraph 6.6 of the 2012 Report, at page 799 B2.)

96. In practice, all the agencies that are empowered to conduct interception (including all the Intelligence Services) have arrangements in place to report errors that arise in their interception operations to the Commissioner. The reported errors are addressed in the Commissioner's annual reports. In his 2013 Annual Report, the Commissioner explained that one of the objectives of his inspections was to ensure that any errors are reported to him (see paragraph 3.29, at page 861 B2), and further stated that, in his experience, the interception agencies "are keen to come forward and report to my office any instances which they judge to be errors" (paragraph 3.59, at page 867 B2). The 2013 Annual Report addresses the reported errors, and suggests various improvements, in paragraphs 3.58-3.68 (pages 867 to 869 B2).

97. I respectfully suggest that the above shows the care and rigour with which the Commissioner performs his oversight role, and makes clear his practical value as an independent safeguard within the RIPA interception regime.

98. Overall, the Commissioner concluded as follows in his 2013 Annual Report:

> "Our inspections and investigations lead me to conclude that the Secretaries of State and the agencies that undertake interception operations under RIPA 2000 Chapter I Part I do so lawfully, conscientiously, effectively and in the national interest. This is subject to the specific errors reported and the inspection recommendations. These require attention but do not materially detract from the judgment expressed in the first sentence." (Page 870 B2.)

99. The Commissioner also found that the provisions of Part I of RIPA "are properly understood and operated by those who are engaged in their operation" and that this

has included "successive Secretaries of State and their relevant officials" (paragraph 6.5.3, at page 897 B2).

Oversight by the Interception of Communications Commissioner of sections 15 and 16 arrangements

100. Section 15 of RIPA imposes a duty on the Secretary of State to ensure, in relation to section 8(4) warrants, that such arrangements are in force as he considers necessary for securing that the requirements of sections 15(2)-(3) and 16 are satisfied. Chapter 6 of the current Code expands on the nature of the required safeguards, as does the revised draft Code to which I refer in paragraph 161 below (which was published for consultation and remains in the public domain). Beyond these public statements, the full details of the sections 15 and 16 arrangements are (and have always been) kept confidential. I have reviewed the safeguards that have been put in place for the purposes of sections 15 and 16 and I am satisfied that they cannot safely be put into the public domain without undermining the effectiveness of interception methods. This would be contrary to the interests of national security and prejudicial to the prevention and detection of serious crime. Interception techniques form a critical resource for the Government in countering terrorism and serious crime. To maintain the effectiveness of the techniques of interception that are adopted, the Government must take steps to ensure appropriate levels of secrecy not only as regards the fact of interception but also as regards the detailed manner in which it is performed. This applies to what I am able to say about the nature of the s. 8(4) regime and the safeguards that attach to it.

101. Although the full details of the sections 15 and 16 arrangements cannot be made public, they are not simply an internal Government matter. Rather, they are made available to the Commissioner (see paragraph 6.1 of the Code) who is required (by section 57(2)(d)(i) of RIPA) to keep them under review. Further, to facilitate oversight by the Commissioner (i) each intercepting agency is required to keep a record of the arrangements in question (see paragraph 5.17 of the Code) and (ii) any breach of the arrangements must be reported to the Commissioner (paragraph 6.1 of the Code).

102. As to the latter, paragraph 3.64 of the 2013 Annual Report (page 869 B2) makes reference to reported errors in the discharge of the duties under sections 15 and 16 of

RIPA and, as is made clear in paragraph 6.5.42 of that Report (page 904 B2), these include instances where the section 16 arrangements were not fully complied with.

103. The then Commissioner's advice and approval was sought and given in respect of the documents constituting the sections 15 and 16 arrangements either before or shortly after 2 October 2000, when RIPA came into force (see paragraph 15 of the Commissioner's 2000 Annual Report at page 434 B2 tab 1). In paragraph 56 of his 2001 Annual Report (see page 455 B2 tab 2), the Commissioner commented as follows:

> "I have been impressed by the care with which these documents have been drawn up, reviewed and updated in the light of technical and administrative developments. Those involved in the interception process are aware of the invasive nature of this technique, and care is taken to ensure that intrusions of privacy are kept to the minimum. There is another incentive to agencies to ensure that these documents remain effective in that the value of interception would be greatly diminished as a covert intelligence tool should its existence and methodology become too widely known. The section 15 and 16 requirements are very important. I am satisfied that the agencies are operating effectively within their safeguards."

104. The sections 15 and 16 arrangements have been updated from time to time since the 2001 Annual Report. When this occurs, the updates are made available to the Commissioner and the Secretary of State. In addition, the advice of the Commissioner is in practice sought when any substantive change is proposed to the sections 15 and 16 arrangements.

105. In 2013, the current Commissioner conducted a detailed investigation into the arrangements for the retention, storage and destruction of interception material and related communications data, in the light of the requirements of section 15(3) of RIPA and in order to determine the extent of the intrusions into privacy that are entailed by current arrangements (see paragraphs 3.48-3.57 of the 2013 Annual Report, at B2 tab 14 pages 865 to 867). The Commissioner explained in his 2013 Annual Report that as part of this detailed investigation he would require steps to be taken to achieve compliance, insofar as he found current arrangements to be wanting.

106. The Commissioner's findings following this detailed investigation included the following:

"• none of the interception agencies retain and store for more that [sic] a short period the contents of intercepted communications which do not relate to a warranted target or which are of no legitimate interest ....

• as to the content of communications which do relate to a warranted target and which are of legitimate intelligence interest, retention periods ... vary depending on the legitimate intelligence use to which this may be put. But section 15(3) of [RIPA] applies to it and my investigations have satisfied me that its provisions are properly observed ...." (Paragraph 5.53.)

"What this investigation has demonstrated is that indiscriminate retention for long periods of unselected intercepted material (content) does not occur. If it did, it would be a breach of section 15(3) of [RIPA]. The interception agencies delete intercepted material (if it is retained at all) after short periods, and in accordance with section 15(3) of [RIPA]." (Paragraph 3.55.)

107. As is made clear in paragraph 6.5.43 of the 2013 Annual Report (page 904 B2 tab 14), the above applies equally to interception operations under section 8(4) warrants.

108. More generally, and as is made clear in Figure 2 in the 2013 Annual Report (page 864 B2), the Commissioner made a number of recommendations in relation to the arrangements under both section 15 and 16 of RIPA, in the light of his recent inspections.

109. The Commissioner's investigation into the retention of communications data remains ongoing (see paragraph 3.56 of the 2013 Annual Report, at page 867 B2).

The Commissioner's investigation into the media disclosures and resulting public concerns

110. As explained in paragraph 5.1-5.3 of the 2013 Annual Report (page 891 B2), the Commissioner has undertaken "extensive investigations" into the subject matter of the media disclosures said to derive from Edward Snowden, insofar as they concern allegations of interception by UK agencies. As is clear from paragraph 5.2, these investigations are underpinned by the Commissioner's statutory duty to report to the Prime Minister any unlawful activity on the part of the interception agencies under Part I of RIPA (should he find that to have occurred). In undertaking these extensive investigations the Commissioner's objectives were twofold (see paragraph 5.3):

"• to investigate and be able to report on the lawfulness (or otherwise) of relevant interception activities which UK interception agencies may undertake or have undertaken.

- to address and report on a variety of concerns which have been expressed publicly in Parliament or in the media arising out of the media disclosures ...."

111. Among other matters, the Commissioner investigated whether Part I of RIPA was "fit for its required purpose in the developing internet age" (see Question 5 in Chapter 6 of the 2013 Annual Report, at page 897 B2).

112. Overall, the Commissioner rejected the charge that the section 8(4) process had become "unfit for purpose in the developing internet age" (paragraph 6.5.55, at page 907 B2).

113. As part of his consideration of this question, the Commissioner observed that during interception under a section 8(4) warrant, the volume of digital data that is obtained is first reduced by filtering, and that:

> "What is filtered out at this stage is immediately discarded and ceases to be available. What remains after filtering (if anything) will be material which is strongly likely to include individual communications which may properly and lawfully be examined under the section 8(4) process. Examination is then effected by search criteria constructed to comply with the section 8(4) process."

114. The Commissioner further concluded that the section 8(4) procedure did not give rise to an improper invasion of privacy (paragraph 6.5.42, at page 904 B2), for various reasons, including (see paragraph 6.5.43):

"• it cannot operate lawfully other than for a statutory purpose. Indiscriminate trawling is not a statutory purpose;

....

• examination of intercepted material has to be in accordance with the certificate such that indiscriminate trawling is unlawful;

....

• the examination of the intercepted material is effected by search criteria constructed to comply with the section 8(4) process ...."

115. As regards the risk of misuse of the section 8(4) process, the Commissioner observed at paragraph 6.5.44 (page 905 B2):

"• I have personally undertaken a detailed investigation of the statutory, technical and practical operation of section 8(4) warrants;

- I have confirmed that the interception agencies understanding of the relevant statutory and Code of Practice requirements coincides with mine as expressed in this report;
- I have confirmed that the interception agencies technical and practical operation of the section 8(4) process is designed to comply with the statutory and Code of Practice requirements;
- I have also made visits to and had meetings with a number of CSPs to discuss and, so far as I am able, understand the technicalities of their implementation of section 8(4) warrants under section 11 of RIPA 2000. The technicalities are complicated and sophisticated but I believe that I have sufficiently understood their principles at least for present purposes."

116. The Commissioner also investigated the interception of internal communications as part of the section 8(4) process. He stated that he was "satisfied from extensive practical and technical information provided to me that it is not at the moment technically feasible to intercept external communications without a risk that some internal communications may also be initially intercepted" (paragraph 6.5.52, at page 906 B2). The Commissioner further noted that the extent to which internal communications may be lawfully examined was "strictly limited" by the safeguards in section 16, and confirmed that the "volume of internal communications lawfully intercepted is likely to be an extremely small percentage of the totality of internal communications and of the total available to an interception agency under a section 8(4) warrant" (paragraph 6.5.54).

117. The Commissioner also investigated whether "the interception agencies misuse their powers under RIPA 2000 Part I Chapter I to engage in random mass intrusion into the private affairs of law abiding UK citizens who have no actual or reasonably suspected involvement in terrorism or serious crime" and whether - if the answer to that question were no – "there [is] any material risk that they or somebody might be able to intrude in this way." (see Question 6 in Chapter 6 of the 2013 Annual Report, at page 908 B2).

118. The Commissioner's answer to the former question was "emphatically no" (paragraph 6.6.2, at page 908 B2). As the Commissioner stated at paragraph 6.6.3:

> "In the real world, intrusion in this context into the privacy of innocent persons would require sentient examination of individuals' communications. The legislation only permits this to the extent that it is properly authorised under the statutory structure which I have described and for the necessity purposes which the legislation

permits. None of this is 'random' or 'mass' and none of it is directed to intrude into the private affairs of law abiding UK citizens."

119. The Commissioner similarly observed at paragraph 6.6.5 (page 909 B2):

> "• individual analysts may have to listen to or look at on screen whatever comes before them, be it relevant to an investigation or not. They are experienced and trained to identify quickly and isolate items of legitimate intelligence interest and to deal with them appropriately;
> • material which is of no intelligence interest is very quickly passed over, as often as not without being read or listened to. In many systems it is immediately marked for deletion. The deletion will then very soon happen, in many systems automatically;
> • meanwhile the analyst, being only human and having a job to do, will have forgotten (if he or she ever took it in) what the irrelevant communication contained. I have sat next to analysts and heard or seen this happening;
> • any assessment of the degree of real intrusion should appreciate that this is what inevitably happens on the ground. The active intrusion is insignificant;
> ...."

120. It is also relevant to note, in this regard, that at paragraph 6.7.5 the Commissioner stated:

> "I am ... personally quite clear that any member of the public who does not associate with potential terrorists or serious criminals or individuals who are potentially involved in actions which could raise national security issues for the UK can be assured that none of the interception agencies which I inspect has the slightest interest in examining their emails, their phone or postal communications or their use of the internet, and they do not do so to any extent which could reasonably be regarded as significant." (Page 913 B2.)

121. The Commissioner is to investigate further the actual application of individual selection criteria to intercepted material (see paragraphs 6.6.8(3) and 6.6.9, at page 910 B2).

122. The 2013 Annual Report addresses whether there is a risk of unlawful intrusions into people's privacy at paragraphs 6.6.10-6.6.18 (pages 911 to 912 B2), as follows:

> "**6.6.10** .... Conceivably possible candidates for effecting such unlawful intrusion could be:
>
> • the Government;
> • one or more of the interception agencies themselves;
> • one or more rogue individuals within the interception agencies; or

- by means of aggressive external cyber attack.

6.6.11 The Government. There is, in my judgment, no risk that the Government would or could require the interception agencies to undertake activity which would be unlawful under RIPA 2000 Part I ....

6.6.12 Successive Secretaries of State have undertaken their statutory functions of granting warrants under RIPA 2000 Part I Chapter I conscientiously, with complete integrity in the public interest, and without any partisan motive which the lawful subject matter would never embrace anyway.

6.6.13 Secretaries of State do not initiate applications for interception warrants. They respond to applications from the interception agencies which are intended to support their operations. Some of these operations are in general response [sic] to intelligence policy priorities of the Joint Intelligence Committee, but these cannot and do not translate into interception applications which are outside the Chapter I statutory necessity purposes.

6.6.14 The Interception Agencies. Unlawful and unwarranted intercept intrusion of any kind, let alone 'massive unwarranted surveillance', is not and, in my judgment could not be carried out institutionally within the interception agencies themselves. The interception agencies and all their staff are quite well aware of the lawful limits of their powers. Any form of massive unwarranted intercept intrusion would as a minimum require a significant unlawful internal conspiracy which would never go undetected, let alone be concealed from external observation or inspection. It would, for instance, require one or more forged interception warrants or certificates and probably unlawful complicity by CSPs. I reckon that the interception agencies and the CSPs would rightly feel offended that the question needs to be asked.

6.6.15 At a more detailed level, possible unwarranted intrusion cannot happen in the abstract. As I have said, a large body of unfiltered data is useless. An individual or group of individuals cannot possibly have sentient access to a single minute's amount of unfiltered UK communications, let alone communications over any longer period. A progressively selected tiny part of this is needed to make possible any examination by a person upon specific individualised inquiry. This is precisely what sections 8(4) and 16 of RIPA 2000 Part I permit. This, and only this, is what happens.

6.6.16 No one sits in front of a computer screen aimlessly trawling through unselected intercepted material. All searches are for a specific authorised purpose. Any more generic computerised search of stored material for intrusive purposes would be unlawful. But any even theoretical possibility of this is heavily moderated by the facts that:

- such material as is stored is required by section 15(3) to be deleted as soon as there are no longer grounds for retaining it as necessary for any of the authorised purposes;
- the filter process necessarily discards large quantities of material which are irrelevant to the interception agencies lawful activities. What remains for any period before it is destroyed is scarcely amenable to mass intrusive surveillance;

- I have carried out the detailed survey of the Retention, Storage and Destruction arrangements of all the interception agencies with powers to apply for interception warrants (see paragraphs 3.48 to 3.57 of this report) with the results which I have described.

6.6.17 A rogue individual or small group. There remains the conceivable, but highly improbable, possibility of small scale unauthorised and unlawful intrusion within the interception agencies by a malign rogue individual or small group. I need to do further detailed research here (see paragraphs 6.6.8 to 6.6.9) and will report in due course, not least to give assurance to the individuals who operate these systems that the work that they do has proper and sufficient protective safeguards.

6.6.18 External cyber attack. This is conceivable, but not within my direct sphere of responsibility or experience. In so far as it might be technically possible - which I simply do not know - I am sure that the interception agencies take proper and appropriate precautions."

123. Overall, and subject to the further research to which the Commissioner referred in paragraph 6.6.17 of his 2013 Annual Report, he concluded that there is "no material risk" that unlawful intrusion into privacy might occur in the operation of the section 8(4) regime (page 915 B2).

124. Finally, I note that the Commissioner investigated a version of the allegation which the ISC had previously investigated (see paragraphs 72-74 above), namely that "British intelligence agencies receive from US agencies intercept material about British citizens which could not lawfully be acquired by intercept in the UK and vice versa and thereby circumvent domestic oversight regimes". The Commissioner rejected this allegation in the light of his investigation (see Question 8 and paragraphs 6.8.1-6.8.6 at page 914 B2).

125. I respectfully agree with and endorse all the above findings of the Commissioner in his 2013 Annual Report.

IV. ADDITIONAL ISSUES REGARDING RIPA INTERCEPTION

The definition of external communications

126. In this section of the statement, I will address the meaning of the term "external communications". In order to address the Claimants' concerns, I will then provide examples of how the definition operates in the context of some common uses of the

internet, such as a Google search, a Facebook post, or a "tweet" on Twitter. I will then go on to explain that in practice, and as envisaged by the section 8(4) regime taken in its entirety, the application of this definition at the point of interception has less importance than its application at the point of selection for examination, where the substantive interference with privacy arises.

127. The term "external communication" is defined in section 20 of RIPA to mean "a communication sent or received outside the British islands". In addition, paragraph 5.1 of the Code provides (at page 372 tab 19 B1):

> "[External communications] include those [communications] which are both sent and received outside the British Islands, whether or not they pass through the British Islands in course of their transit. They do not include communications both sent and received in the British Islands, even if they pass outside the British Islands en route."

128. Most internet communications between individuals are not transmitted directly from the sender to the recipient. An email, for instance, will normally be routed from the sender's computer to the email server of their internet service provider ("ISP"), from there to the recipient's ISP's email server, and from there to the recipient's computer. Where both the sender and recipient are in the British Islands and use email services provided by UK-based ISPs, these emails will have IP addresses (that is, Internet Protocol addresses: in simple terms the "address" of a computer on the internet) that are within the British Islands on all legs of their journey. However, many individuals in the British Islands use webmail services, such as Hotmail, Gmail and Yahoo!, which use servers that are not located in the British Islands. A message from an individual in the British Islands using Gmail to another individual in the British Islands using Yahoo! may well be routed first from a IP address within the British Islands to a US IP address; secondly from that US IP address to an Irish IP address; and finally from the Irish IP address to a IP address within the British Islands.

129. The distinction in paragraph 5.1 of the Code between (i) the routing of a communication and (ii) the location from which it is sent / where it is received is intended to address these different factual scenarios, and to indicate that the route that a message takes is immaterial. A "communication" for these purposes, both in RIPA and the Code, has both a particular sender and a particular recipient. Under paragraph 5.1 of the Code, the relevant question to ask is not via whom (or what) a message has been transmitted, but for whom (or what), objectively speaking, the message is

intended. Thus, an email from a person in London to a person in Birmingham will be an internal, not external, communication for the purposes of RIPA and the Code, whether or not it is routed via IP addresses outside the British Islands, because the intended recipient is within the British Islands. The intended recipient is not any of the servers that handle the communication whilst en route (whether that server be located inside, or outside, the British Islands). Indeed, the sender of the email cannot possibly know at the time of sending (and is highly unlikely to have any interest in) how that email is routed, or what servers will handle it on its way to the intended recipient.

130. This issue was addressed during the course of the Parliamentary debates on the Regulation of Investigatory Powers Bill. As Lord Bassam of Brighton made clear in Lords Committee (Hansard, 12 July 2000 at column 323), an email message from one person in London to another in Birmingham would be an internal communication, whatever route it took to reach its destination, and via whatever ISP servers it passed on the way (page 424 tab 21 B1):

> "It is just not possible to ensure that only external communications are intercepted. That is because modern communications are often routed in ways that are not all intuitively obvious.... An internal communication–say, a message from London to Birmingham–may be handled on its journey by Internet service providers in, perhaps, two different countries outside the United Kingdom. We understand that. The communication might therefore be found on a link between those two foreign countries. Such a link should clearly be treated as external, yet it would contain at least this one internal communication. There is no way of filtering that out without intercepting the whole link, including the internal communication."

131. The possibility that internal communications may be routed outside the British Islands is of course one which the operation of the internet brings into particularly sharp focus. But it is not in any way a new issue, or one which arose only with the advent of the internet. It is quite possible, for example, for a letter sent from one person in the British Islands to another person in the British Islands to pass outside the British Islands en route: for instance, if it were delivered by an overseas postal operator functioning within the British Islands, which sorted some items of mail outside the British Islands. The Code makes clear that the letter would not be an "external communication", simply because it was handled in the course of its journey by persons outside the British Islands, who were not the intended recipient of that letter.

132. It may assist if I explain how the definition of "external communications" in the Code would apply, on the same principles explained at paragraph 129 above, in other common factual scenarios involving the use of the internet, such as a Google search, a search of YouTube for a video, a "tweet" on Twitter, or the posting of a message on Facebook.

133. A person conducting a Google search for a particular search term in effect sends a message to Google asking Google to search its index of web pages. The message is a communication between the searcher's computer and a Google web server (as the intended recipient). The Google web server will search Google's index of web pages for search results, and in turn send a second communication – containing those results - back to the searcher's computer (as the intended recipient).

134. Google's data centres, containing its servers, are located around the world; but its largest centres are in the United States, and its largest European centres are outside the British Islands. So a Google search by an individual located in the UK may well involve a communication from the searcher's computer to a Google web server, which is received outside the British Islands; and a communication from Google to the searcher's computer, which is sent outside the British Islands. In such a case, the search would correspondingly involve two "external communications" for the purposes of section 20 of RIPA and paragraph 5.1 of the Code.

135. Similarly, a computer user in the British Islands searching for a video posted on YouTube will in effect send a communication to YouTube's website to ask it to give him the results of a particular search; which means that he communicates with a YouTube web server; and the web server, in turn, communicates back to him the results of the search that he has made. Whether or not those communications are "external" will depend upon where the web server used by YouTube is located.

136. Making a post on Facebook, or "tweeting" on Twitter, entails placing a message upon a web-based platform, in order that it can be seen by a wide audience. In such a case, the recipient of the relevant "communication" is not any particular person who eventually reads the post or tweet, whose exact identity the person posting or tweeting cannot possibly know at the time the message is sent. Rather, it is the platform itself, because the platform is both the repository for the message, and the means by which it is broadcast to those with access to the relevant Twitter account or Facebook page.

137. Thus a user located in the British Islands posting a message on Facebook will communicate with a Facebook web server, located in a Facebook data centre. If the Facebook data centre is outside the British Islands, then the message will be an "external communication". (It is also possible to use Facebook to send an email to an individual: and in such a case, the recipient of the communication would be that individual himself; and – as in the case of other types of email - whether or not the communication was internal or external would depend upon where that individual was located but not on how the email was routed.)

138. Similarly, a user located in the British Islands posting a message on Twitter will communicate with a Twitter web server forming part of Twitter's data centre infrastructure. That data centre infrastructure is largely based in the United States; so the communication may well be "external" for the purposes of RIPA and the Code.

139. As Lord Bassam made clear, interception under the s. 8(4) regime takes place at the level of communications cables, rather than at the level of individual communications. These cables carry large quantities of communications which are likely to consist of a mixture of external and internal communications. Knowledge of the way in which traffic is routed over the internet enables section 8(4) interception to be targeted at those communications links that maximise the opportunity of acquiring external communications meeting the descriptions of material certified under section 8(4)(b)(i) of RIPA. But the section 8(4) regime envisaged this "mixing" of external and internal communications in communications cables, and a section 8(4) warrant may authorise the interception of communications that are not external communications insofar as such interception is "necessary" under section 5(6)(a). Despite the fact that some UK to UK communications may be intercepted under section 8(4) warrants and that common uses of the internet by persons in the British Islands, such as a Google search, a Facebook post, or a "tweet" on Twitter, may entail the making of "external communications" for the purposes of Chapter I of RIPA, the section 8(4) regime as a whole is designed so as not to authorise the selection for examination of communications of this nature, except in the tightly constrained circumstances set out in section 16 of RIPA. It is therefore unlikely that such communications would be capable of being read, looked at or listened to, even in the unlikely event (see paragraph 157 below) that they fell within a description of communications to which a section 8(4) warrant related.

140. By section 16(1)(a) of RIPA, before such communications can be examined, they must consist of material of a class falling within a certificate issued by the Secretary of State, the examination of which is necessary for the purposes set out in section 5(3) of RIPA. Further, by section 16(1)(b) of RIPA, they must also be selected to be examined otherwise than according to a factor relating to an individual who is known to be for the time being in the British Islands, and which has as its purpose, or one of its purposes, the identification of material contained in communications sent by him, or intended for him (save in the limited circumstances set out in sections 16(3)-(4) of RIPA).

141. In practice, this means (for example) that if the content of a Google search made by an individual known to be in the British Islands had been intercepted pursuant to an interception warrant under section 8(4) of RIPA, it could not be selected to be read, or even looked at, on the basis of any factor referable to that individual (save in the limited circumstances set out in sections 16(3)-(4)).

Interception under section 8(1) and section 8(4) warrants

142. The section 8(4) warrant system was designed by the Government, and enshrined in law, to take account of practical considerations relating to the interception of external communications, whilst complying with the provisions of Article 8 of the Convention and ensuring that proper control is exercised over (i) those who could have access to intercepted material; (ii) to what material access would be authorised; and (iii) what should happen to the intercepted material (both that which is accessed by officials of the Intelligence Services and that which is not).

143. Unlike the section 8(1) regime, the section 8(4) regime does not require a person or set of premises to be named or described in the interception warrant. There are important practical differences between gathering intelligence on individuals and organisations within the British Islands and gathering intelligence on individuals and organisations that operate outside that jurisdiction (see §§217-221 of the Open Response). If a section 8(1)-type regime were to be applied to the interception of external communications, the probability of obtaining any or any adequate intelligence about individuals and organisations operating outside the British Islands would be greatly reduced.

144. Within the British Islands, the Government has sufficient control and considerable resources to investigate individuals and organisations, and it is feasible to adopt an interception regime that requires either a particular person, or a set of premises, to be identified before interception can take place. Outside the British Islands, the Government does not have the same ability to identify either relevant individuals or premises. For example, the Government is in many cases not aware of the precise location and online identities of members of Al-Qaeda around the world, or of cyber criminals, Taleban insurgents, proliferators of weapons of mass destruction or precursor chemicals, or of other similar individuals or organisations whose activities pose a threat to national security, the prevention and detection of serious crime or the economic well-being of the United Kingdom. And even if the Government were aware of their precise location and online identities, it would be unlikely to have the same practical ability to access communications relating to those individuals or premises. For example, it may very well not be possible to target communications systems carrying communications from such individuals or organisations outside the British Islands in circumstances where those systems are operated by overseas communications service providers who are not providing services to individuals within the British Islands.

145. A simple illustration of the difficulties that arise may assist. Suppose that the Government wished to intercept electronic communications from particular premises in the UK. For example, a reliable Security Service covert human intelligence source ("CHIS") might report that a computer at certain UK premises (such as a house) was being used by Islamic extremists to send emails related to terrorist attack planning to individuals located in Pakistan, who were associated with Al Qaeda. The Security Service has a number of tools short of interception to be able to identify the occupants of the house, and therefore the potential users of the email account:

(a) The Security Service can search against open source information such as the electoral roll, telephone directories and companies databases to identify the occupants.

(b) The Security Service can also enquire with the local police force, to see whether the address is known to them (for example, whether it is on the Police National Computer).

(c) The Security Service can deploy surveillance against the address and take photographs of the occupants, subject to a Directed Surveillance Authorisation under section 26(2) of RIPA. Those photographs could then be shown to the existing Security Service CHIS to determine whether the occupants were known to the CHIS.

(d) The Security Service can apply to major telephone and internet service providers within the UK under Chapter 2 of Part I of RIPA for a "subscriber check" for the property to determine the name of the subscriber for any telephone and broadband lines at the property.

146. Once the broadband line at the property had been identified, the Security Service would then be able to apply to the Secretary of State for a warrant under section 8(1) of RIPA to intercept that line. Analysis of the product from the interception of the broadband line would reveal the email accounts used by the extremists to communicate. The Security Service could then apply for a further RIPA section 8(1) warrant to intercept the operational email accounts directly.

147. By contrast, even in the unlikely event that the Government knew the location of the equivalent premises abroad, it may very well have neither the same practical ability to identify the apparatus over which those communications were to be carried; nor the same practical power to obtain messages from that apparatus, even if it were identified.

148. Once travelling over the internet, the route whereby an electronic message reaches its intended recipient can be almost infinitely varied. The nature of the internet is that messages will be routed by the most efficient route available at the time. That route will not necessarily be the route that is geographically the shortest. It will be determined by a number of factors, including the cost of transmission via a specific route; the number of links between the start point and end point for the message; and the volume of traffic passing over particular parts of the internet at particular times of day.

149. Taking these considerations in the round, it will be apparent that the only practical way in which the Government can ensure that it is able to obtain at least a fraction of the type of communication in which it is interested is to provide for the interception of

a large volume of communications, and the subsequent selection of a small fraction of those communications for examination by the application of relevant selectors.

150. I understand the Complainants have not suggested that other signatories to the Convention do not make use of surveillance regimes that, like the United Kingdom's section 8(4) regime, involve the interception of volumes of communications and the subsequent performance of a process of selection with respect to those communications to obtain material for further consideration by government agencies. As has already been noted at §219.2 of the Open response, German law permits what is termed "strategic monitoring", which involves the interception of communications channels as a whole and the subsequent filtering of the intercepted data using selection terms. Strategic monitoring is clearly similar to interception under the section 8(4) regime.

151. Accordingly, I would respectfully suggest that the section 8(4) regime was, during the relevant period, an appropriate practical means by which intelligence relating to individuals and organisations operating abroad could be gathered. Any regime that, like the section 8(1) regime, only permitted interception in relation to specific persons or premises, would not have allowed adequate levels of intelligence information to be obtained and would not have met the undoubted requirements of intelligence for the protection of national security.

Internal communications intercepted under the section 8(4) regime

152. I am advised that it has been suggested by Liberty that (i) a high proportion of communications that are not external communications are carried over international cables and that (ii) such communications will also be intercepted under the section 8(4) regime (§84 of Liberty's Grounds of Claim). I can neither confirm nor deny the specific factual bases of this argument. But I can confirm that a section 8(4) warrant may authorise the interception of communications that are not external communications insofar as such interception is "necessary" under section 5(6)(a).

153. There are a number of reasons why as a matter of practice the section 8(4) regime may need to be able to intercept more than simply those communications that may – pursuant to section 16 and the certificate in question – be read, looked at or listened to. In particular, internet communications may take any number of routes to get from

sender to recipient. Internal and external communications will be carried together over communications links and it is not at all unusual for internal communications to be routed over international links. While it is a straightforward matter to distinguish between external and internal communications in the case of fixed-line telephony, this is considerably more difficult when it comes to mobile telephony, and in particular internet communications.

154. Thus, when conducting interception under a section 8(4) warrant, knowledge of the way in which communications are routed over the internet is combined with regular surveys of internet traffic to identify those bearers that are most likely to contain external communications that will meet the descriptions of material certified by the Secretary of State under section 8(4)(b)(i) of RIPA. While this approach may lead to the interception of some communications that are not external, section 8(4) operations are conducted in a way that keeps this to the minimum necessary to achieve the objective of intercepting wanted external communications.

155. Section 5(6)(a) makes clear that the conduct authorised by a section 8(4) warrant may in principle include the interception of communications which are not external communications insofar as that is necessary in order to intercept the external communications to which the warrant relates. But the primary purpose and object of any conduct authorised or required by a section 8(4) warrant must consist in the interception of external communications.

156. As the Commissioner concluded in his 2013 Annual Report, following an "in detail" investigation of the relevant (and sensitive) technical background relating to the section 8(4) procedure:

> "... at present there are no other reasonable means that would enable the interception agencies to have access to external communications which the Secretary of State judges it is necessary for them to obtain for a statutory purpose under the section 8(4) procedure." (Paragraph 6.5.51, at page 906 tab 14 B2.)

157. The section 8(4) warrant regime accordingly takes account of practical considerations relating to the interception of external communications whilst ensuring that access to the intercepted material is strictly controlled and regulated. So far as the latter is concerned, it is important to note the significant distinction between the act of interception itself, and a person actually reading, looking at or listening to intercepted

material. Communications intercepted under the section 8(4) regime cannot be read, looked at or listened to by anyone except in accordance with the certificate and pursuant to section 16 of RIPA and section 6(1) of the Human Rights Act 1998. In addition, sections 16(3)-(5A) strictly limit the circumstances in which intercepted material may be selected for examination according to a factor referable to an individual known for the time being to be in the UK.

158. In summary, while a section 8(4) warrant may therefore authorise the interception of some communications transmitted between two individuals in the UK where such interception is necessary under section 5(6)(a), I am satisfied that none of these communications should be selected to be read, looked at or listened to by any person, save under the strictly limited circumstances set out above.

Amendments to the Code

159. The Code is issued by the Secretary of State under section 71 of RIPA. That section requires the Secretary of State to publish a draft code before it is issued, and to consider any representations made about the draft. Published drafts (amended, as appropriate, in the light of the consultation) must then be laid before both Houses of Parliament, and the Code is brought into force in accordance with an order subject to the affirmative procedure.

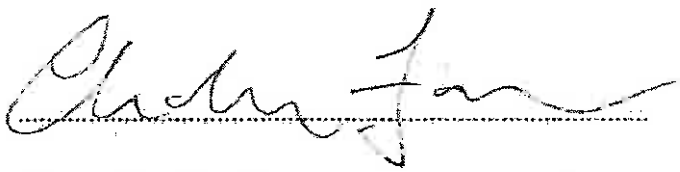
160. The version of the Code that is currently in force was first brought into force in 2002 (and was last published in 2007).

161. In March 2010, the Home Office published on its website a revised draft of the Code (see B1 tab 20 page 392). The draft was subject to a targeted consultation, lasting three months. The aim, in response to the *Liberty v UK* judgment, was to make public, to the extent possible, further information as to how material gathered under a section 8(4) warrant comes to be examined following interception. The proposed changes were mainly to chapters 5 and 6. Some minor corrections and updates were also made.

162. Three consultation responses were received and considered by the Home Office. No further revisions were made to the draft Code as a result. The amended Code was, in the event, never brought into force, because of timing constraints and the expectation

that new legislation would be enacted relating to communications data, which would in turn have required further changes to all the relevant RIPA codes of practice.

I believe the facts stated in this witness statement are true.



Charles Blandford Farr

Dated: 16 May 2014