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

THE RESPONDENTS' OPEN RESPONSE

Privacy International and Liberty will be referred to below as "the Claimants".
The term "Respondents" is used below to refer to all Respondents in both Claims.
The term "Intelligence Services" is used below to refer to the three Respondents in Liberty's Claim.

Introduction

1. The two Claims overlap substantially. For convenience, the Respondents are filing a single Open Response to both Claims.

2. This Open Response:

   2.1 Summarises the need for the "neither confirm nor deny" policy, and explains its operation in the present case (§§5-10; **Part I**).

   2.2 Summarises the value of intelligence sharing with foreign States

(including the US Government), and the value of lawful interception (§§11-14; **Part I**).

2.3 Addresses the Tribunal's procedural regime, insofar as is relevant to the present Claims (§§15-25; **Part II**).

2.4 Insofar as the Claims concern the US Prism programme / alleged "upstream collection" by the US Government (**Part III**):

(a) sets out the Respondents' open position on the factual allegations made (§§26-35);

(b) sets out the relevant domestic legal regime ("the Intelligence Sharing regime") (§§36-76);

(c) identifies the pure issues of law that, pursuant to the Tribunal's procedural ruling of 22 January 2003 in IPT/01/62 and IPT/01/77 ("the Procedural Ruling"), are suitable for determination at a public *inter partes* hearing ("a Legal Issues Hearing") (§§77-79); and

(d) sets out the Respondents' position on those pure issues of law (§§8096).

2.5 Insofar as the Claims concern the alleged "Tempora" interception operation (**Part IV**):

(a) sets out the Respondents' open position on the factual allegations made (§§97-101);

(b) sets out the relevant domestic legal regime ("the s. 8(4) regime") (§§102-178)[1];

(c) identifies the pure issues of law that are suitable for determination at Legal Issues Hearing (§§179-182); and

(d) sets out the Respondents' position on those pure issues of law (§§183-221).

2.6 Suggests directions for the future management of these two Claim (§§222-225; **Part V**).

3. A list of the pure issues of law, and the Respondents' position on each them, is in the Appendix to this Open Response.

4. The Respondents' overall position is that the Intelligence Sharing Regime and the s. 8(4) regime are compatible with Art. 8 ECHR, and that the latter does not unlawfully discriminate against any person or persons. The Claims

[1] Liberty also raises the possibility that the alleged "Tempora" operation also is based in part on ss. 1(5)(c) and 22(5) of RIPA. See §98 below.

should therefore be dismissed.

I. THE FACTS APPLYING TO BOTH PRISM AND TEMPORA CLAIMS

The "neither confirm nor deny" policy, and its operation in the present case

5. Secrecy is essential to the necessarily covert work and operational effectiveness of the Intelligence Services, whose primary function is to protect national security. See *e.g. Attorney General v. Guardian Newspapers Ltd (No.2)* [1990] 1 AC 109, *per* Lord Griffiths at 269F.

6. As a result, the mere fact that the Intelligence Services are carrying out an investigation or operation in relation to say, a terrorist group or hold information on a suspected terrorist will itself be sensitive. If, for example, a hostile individual or group were to become aware that they were the subject of interest by the Intelligence Services, they could not only take steps to thwart any (covert) investigation or operation but also attempt to discover, and perhaps publicly reveal, the methods used by the Intelligence Services or the identities of the officers or agents involved. Conversely, if a hostile individual or group were to become aware that they were not the subject of Intelligence Service interest, they would then know that they could engage or continue to engage in their undesirable activities with increased vigour and increased confidence that they will not be detected.

7. In addition, an appropriate degree of secrecy must be maintained as regards 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 acquire detailed information on such matters then they will be able to adapt their conduct to avoid, or at least minimise, the risk that the Intelligence Services will be able successfully to deploy those capabilities and techniques against them.

8. It has thus been the policy of successive UK Governments to neither confirm nor deny whether they are monitoring the activities of a particular group or individual, or hold information on a particular group or individual, or have had contact with a particular individual. Similarly, the long-standing policy of the UK Government is to neither confirm nor deny the truth of claims about the operational activities of the Intelligence Services, including their intelligence-gathering capabilities and techniques.

9. Further, the "neither confirm nor deny" principle would be rendered nugatory, and national security thereby seriously damaged, if every time that sensitive information were disclosed without authority (*i.e.* "leaked"), or it was alleged that there had been such unauthorised disclosure of such information, the UK Government were then obliged to confirm or deny the veracity of the information in question.

10. It has thus 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 UK Government.[2] That long-standing policy is applied in this Open Response.

The value of intelligence sharing with foreign States, and the value lawful interception

11. In order to pursue their statutory objectives, the Intelligence Services need to share intelligence with foreign Governments, including the US Government (with which the Intelligence Services have particularly close ties). 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 terrorists, organised criminals and others seeking to harm national security.

12. Interception under the Regulation of Investigatory Powers Act 2000 ("RIPA") provides both tactical and strategic 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. Strategic information that is obtained via interception is used to reveal the existence of new targets (a significant proportion of initial intelligence leads derive from interception operations), as well as the significance, long term plans, international connections and *modus operandi* 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.

13. Overall, RIPA interception is a critical tool in investigations into the full range of threats to national security. Intelligence from interception has played a vital role in stopping many of the terrorist plots that the Intelligence Services and law enforcement agencies have tackled in the past decade.

14. As the Interception of Communications Commissioner ("the Commissioner") confirmed in the Foreword to his 2012 Annual Report:

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

[2] Such a confirmation would only be given in exceptional circumstances – for example, on the basis either that there were some compelling countervailing public interest in departing from the neither confirm nor deny principle that clearly outweighed the public interest in protecting national security (or on balance promoted the public interest in protecting national security).

II. THE TRIBUNAL'S PROCEDURAL REGIME[3]

15. The Tribunal's procedure is governed by ss. 67-69 of RIPA and the Investigatory Powers Tribunal Rules 2000, SI 2000/2665 ("the Rules"), made under s. 69.

16. In §173 of the Procedural Ruling the Tribunal concluded that r. 9(6) of the Rules[4] was *ultra vires* the rule-making power in s. 69 of RIPA. Further, the Tribunal held that:

    16.1 "purely legal arguments, conducted for the sole purpose of ascertaining what is the law and not involving the risk of disclosure of sensitive information" should be heard by the Tribunal in public (Procedural Ruling, §172); and

    16.2 the Tribunal's reasons for its ruling on any "pure questions of law" (§195) that are raised at such a hearing may be published without infringing either r. 13 of the Rules or s. 68(4) of RIPA[5] (Procedural Ruling, §§190-191).

17. It follows that, where necessary, the Tribunal may hold a Legal Issues Hearing to consider any relevant (and disputed) pure issues of law,[6] and may subsequently publish its rulings (with its reasoning) on such issues.

18. The Tribunal also concluded in the Procedural Ruling that, with the exception of r. 9(6), the Rules are valid and binding (§148). It follows from this conclusion, and from r. 6(2)-(5) of the Rules, that - prior to the determination of a claim[7] - the Tribunal cannot disclose to a claimant anything that a respondent has decided should only be disclosed to the Tribunal, and similarly cannot order a respondent to make such disclosure itself.

19. The overall effect of the Procedural Ruling is thus that:

    19.1 where necessary, the Tribunal first holds a Legal Issues Hearing to determine such relevant pure issues of law as are in dispute between the parties, and publishes its rulings (with reasons) on those pure issues of law;

---

[3] The Tribunal's jurisdiction and remedial powers are addressed below.

[4] R. 9(6) provides:

"*The Tribunal's proceedings, including any oral hearing, shall be conducted in private.*"

[5] The effect of r. 13 and s. 68(4) is in essence that if the claim is dismissed then the Tribunal may only give to the claimant a statement that "*no determination has been made in his favour*", but that if the claim is upheld then the Tribunal may, subject to r. 6(1), provide a summary of its determination, including any findings of fact.

[6] As the Tribunal confirmed in the subsequent case of *Frank-Steiner v. the Data Controller of the Secret Intelligence Service* (IPT/06/81/CH), 26 February 2008, at §5, the pure issues of law can as necessary be considered on the basis of hypothetical facts.

[7] As noted in footnote 5 above, the Tribunal has power - subject to r. 6(1) - to provide a summary of its determination, including any findings of fact, in the event that the overall claim is upheld.

19.2 the Tribunal then investigates the claim in closed session; and

19.3 as necessary,[8] the Tribunal applies its rulings on the pure issues of law to the facts that it has found following its closed session investigation of the claim.

20. This was the approach taken in the two joined cases which gave rise to the Procedural Ruling. Following the Procedural Ruling, the two cases were separated and disputed pure issues of law were identified and determined following Legal Issues Hearings (the ruling on the pure issues of law in IPT/01/77 of 9 December 2004 is considered below). Each claim was then finally determined following the Tribunal's investigation of the cases in closed session. This was similarly the approach taken in *Frank-Steiner v. the Data Controller of the Secret Intelligence Service* (IPT/06/81/CH).[9]

21. The European Court of Human Rights ("the ECtHR") unanimously upheld the Tribunal's procedural regime as summarised above in *Kennedy v. UK* (2011) 52 EHRR 4, at §§184-191. (*Kennedy* arose out of one of the domestic cases that case rise to the Procedural Ruling, namely IPT/01/62.)

22. In the Respondents' submission therefore, the approach set out in §19 above is the one prescribed in the Rules, is tailored to the subject matter of the matters falling within the Tribunal's jurisdiction, has been expressly accepted as fair and compatible with the ECHR by the ECtHR; and should be followed by the Tribunal in the present Claims.

23. Liberty appears to accept this at §§5-8 and 107 of its Grounds of Claim. However, at §§99-106 of its Grounds of Claim, Liberty appears also to be arguing that the Tribunal should adopt some different course, in the light of *Bank Mellat v. HM Treasury (No. 1)* [2013] UKSC 38. *Bank Mellat* was however not concerned with the very particular and specific procedure of the Tribunal. It offers no sound basis for revisiting the Procedural Ruling, as upheld (unanimously) by the ECtHR in *Kennedy*.

24. For its part, Privacy International seeks a public hearing of its Claim. It argues that the existence and scope of the alleged "Tempora" operation is now in the public domain, and that the ordinary policy of "neither confirm nor deny" has no lawful or proper basis in such circumstances (§59 of Privacy International's Statement of Grounds). However, this argument fails to appreciate the ordinary operation of the "neither confirm nor deny" policy in

[8] Following its investigation the Tribunal may *e.g.* find that the respondents have not in fact undertaken any activities in relation to a claimant, with the result that the claim will be dismissed without the need to apply the rulings on the pure issues of law to any specific factual findings.

[9] There is a class of Tribunal cases that have not proceeded in this way (see *e.g. Paton v. Poole Borough Council*, IPT/09/01-05/C, determination of 29 July 2010). But that is because, in these cases, the respondents have decided that the entirety of their factual case can be dealt with in open session, with the result that the Legal Issues Hearing becomes in effect indistinguishable from a substantive hearing on all disputed matters. Where, however, a respondent decides that any part of its factual case is closed, then the approach in §19 applies.

the case of alleged leaks (see §§9-10 above). The long-standing general policy is clear: the "neither confirm nor deny" stance is maintained. In §5 of its letter of 25 October 2013, Privacy International makes various procedural suggestions. However, none of these are advanced by reference to the Rules or the Procedural Ruling, which should be followed.

25. The Respondents are filing a Closed Response with this Open Response. For the avoidance of doubt, the Respondents' position, with respect to the Tribunal, is that in the light of r. 6 of the Rules, the Procedural Ruling and *Kennedy*, nothing in the Closed Response can be disclosed to the Claimants without the Respondents' consent.

III. THE US PRISM PROGRAMME / ALLEGED "UPSTREAM COLLECTION" BY THE US GOVERNMENT

The facts

26. Privacy International's Ground 1 and Liberty's First Ground concern alleged access by the Intelligence Services to information obtained by the US Government via the Prism programme, and (in the case of Privacy International's Ground 1) pursuant to an alleged programme of "upstream collection" (see §§17-18 of Privacy International's Statement of Grounds).

27. Insofar as the relevant intelligence activities and operations of the US Government have been the subject of official statements by the executive branch of the US Government, the Respondents accept the truth of those official statements, and do not seek to adopt a neither confirm nor deny stance in relation to any of their contents. The Respondents adopt a 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 separately confirmed by an official statement by the executive branch of the US Government.[10]

28. The Respondents thus openly accept the existence of Prism, as it has been expressly avowed by the executive branch of the US Government. As the US Director of National Intelligence (Mr James Clapper), confirmed in a statement of 8 June 2013, Prism is 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"). In addition, the National Security Agency's document of 9 August 2013, "*The National Security Agency: Missions, Authorities, Oversight and Partnerships*" 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*

[10] For the avoidance of doubt: an absence of a denial is not an official confirmation for this purpose. (At various points the Claims state that certain news reports have not been "denied" / "disputed" by the US authorities: see *e.g.* §§59-60 of Liberty's Grounds of Claim.)

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 ...." [11] (Original emphasis.)

29. In addition, *The National Security Agency: Missions, Authorities, Oversight and Partnerships* document further confirms that, in its foreign intelligence mission, the National Security Agency "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).

30. Following media reporting on Prism, the Intelligence and Security Committee ("the ISC"; for which, see §§61-68 below) investigated an allegation that GCHQ had acted illegally by accessing communications content via the Prism programme. The ISC published a Statement on this investigation on 17 July 2013. It concluded (among other things) that GCHQ had not "circumvented or attempted to circumvent UK law" (Statement, §6).

31. 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, the Respondents confirm that GCHQ has obtained information from the US Government that the US Government obtained via Prism. However, beyond this confirmation, the Respondents maintain the ordinary "neither confirm nor deny" stance for intelligence matters. Accordingly, they do not provide in this open Response any further indication of the timing, nature or extent of GCHQ's access to

[11] The document cites the example of Section 702 being used in 2009 to identify the Colorado-based Najibullah Zazi, who subsequently pleaded guilty to conspiring to bomb the New York subway system.

information via Prism. Further, and for the avoidance of doubt, the Respondents neither confirm nor deny that either the Security Service or the Secret Intelligence Service ("SIS") has obtained, from the US Government, information that has been obtained under the Prism programme.

32. Save as set out above, the Respondents neither confirm nor deny any of the factual claims in Privacy International's Statement of Grounds and Liberty's Grounds of Claim relating to (i) US intelligence activities / operations, (ii) access, by any of the Intelligence Services, to any information obtained as a result of those US activities / operations or (iii) involvement in those US activities / operations by any of the Intelligence Services.

33. In addition, and for the avoidance of doubt, the Respondents neither confirm nor deny:

    33.1 whether any of the Claimants' communications[12], or any communications data[13] pertaining to those communications, have been obtained by the US Government; and

    33.2 <u>if</u> any such communications or data have been obtained by the US Government, whether any of those communications or data have been obtained by any of the Intelligence Services from the US Government.

34. The Respondents nevertheless accept that the Claimants may challenge the compatibility of the Intelligence Sharing regime with Art. 8 of ECHR on the basis that their communications / communications data might <u>in principle</u> have been obtained by the US Government and might <u>in principle</u> have been obtained by the Intelligence Services from the US Government. Compare *e.g.* §78 of *Weber and Saravia v. Germany* (2008) 46 EHRR SE5.

35. The Claimants cannot however claim to be victims of any Art. 10 interferences. Neither are journalists or news organisations. Their position can thus be distinguished from that of Ms Weber in the *Weber* case, who was a freelance journalist: §§5 and 144-146 of *Weber*. In any event, Art. 10 adds nothing to the analysis under Art. 8.

<u>The Intelligence Sharing regime</u>

36. The Intelligence Sharing regime, relevant to Prism, principally derives from the following statutes:

    36.1 the Security Service Act 1989 ("the SSA") and the Intelligence Services Act 1994 ("the ISA"), as read with the Counter-Terrorism Act 2008 ("the CTA");

---

[12] This term is used in this Response in accordance with its broad meaning in RIPA. Pursuant to s. 81(1) of RIPA a communication includes, among other things, "anything comprising speech, music, sounds, visual images or data of any description".

[13] For the detailed definition of "communications data" and the related definition of "traffic data" see s. 21(4) and s. 21(6) of RIPA, respectively.

36.2 the Human Rights Act 1998 ("the HRA");

36.3 the Data Protection Act 1998 ("the DPA"); and

36.4 the Official Secrets Act 1989 ("the OSA").

37. In addition, the provisions of RIPA are relevant as regards the scope of the power of UK public authorities to obtain communications and/or communications data from foreign intelligence agencies.

The SSA, the ISA and the CTA

38. S. 1 of the SSA provides in relevant part:

> *"(2) The function of the [Security] Service shall be the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means.*
> *(3) It shall also be the function of the [Security] Service to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands.*
> *(4) It shall also be the function of the [Security] Service to act in support of the activities of police forces, the National Crime Agency and other law enforcement agencies in the prevention and detection[14] of serious crime."*

39. The operations of the Security Service are under the control of the Director-General, who is appointed by the Secretary of State (s. 2(1) of the SSA). By s. 2(2)(a), it is the duty of the Director-General to ensure:

> *"...that there are arrangements for securing that no information is obtained by the Service except so far as necessary for the proper discharge of its functions or disclosed by it except so far as necessary for that purpose or for the purpose of the prevention or detection of serious crime or for the purpose of any criminal proceedings..."*

See also s. 19(3) of the CTA.[15]

40. Subject to s. 1(2) of the ISA, the functions of SIS are, by s. 1(1) of the ISA:

> *"(a) to obtain and provide information relating to the actions or intentions of persons outside the British Islands; and*
> *(b) to perform other tasks relating to the actions or intentions of such persons."*

41. By s. 1(2) of the ISA:

---

[14] By s. 1(5) of the SSA, the definitions of "prevention" and "detection" in s. 81(5) of RIPA apply for the purposes of the SSA.

[15] By s. 19(3), information obtained by the Security Service for the purposes of any of its functions "*may be disclosed by it - (a) for the purpose of the proper discharge of its functions, (b) for the purpose of the prevention or detection of serious crime, or (c) for the purpose of any criminal proceedings.*"

"*The functions of the Intelligence Service shall be exercisable only –*

(a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or

(b) in the interests of the economic well-being of the United Kingdom; or

(c) in support of the prevention or detection of serious crime."

42. The operations of SIS are under the control of the Chief of the Intelligence Service, who is appointed by the Secretary of State (s. 2(1) of the ISA). By s. 2(2)(a), it is the duty of the Chief of the Intelligence Service to ensure:

"... that there are arrangements for securing that no information is obtained by the Intelligence Service except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary –

(i) for that purpose;

(ii) in the interests of national security;

(iii) for the purpose of the prevention or detection of serious crime; or

(iv) for the purpose of any criminal proceedings ..."

See also s. 19(4) of the CTA.[16]

43. By s. 3(1)(a) of the ISA, the functions of GCHQ include the following:

"... to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material ...."

44. By s. 3(2) of the ISA, these functions are only exercisable:

"*(a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or*

(b) in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or

(c) in support of the prevention or detection of serious crime."

45. GCHQ's operations are under the control of a Director, who is appointed by the Secretary of State (s. 4(1)). By s. 4(2)(a), it is the duty of the Director to ensure:

"... that there are arrangements for securing that no information is obtained by GCHQ except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or for the purpose of any criminal proceedings ..."

See also s. 19(5) of the CTA.[17]

---

[16] By s. 19(4), information obtained by SIS for the purposes of any of its functions "*may be disclosed by it - (a) for the purpose of the proper discharge of its functions, (b) in the interests of national security, (c) for the purpose of the prevention or detection of serious crime, or (d) for the purpose of any criminal proceedings*."

46. Thus, specific statutory limits are imposed on the information that each of the Intelligence Services can obtain, and on the information that each can disclose. Further, these statutory limits do not simply apply to the obtaining / disclosing of information to other persons in the United Kingdom: they apply equally to obtaining / disclosing information to persons abroad, including foreign intelligence agencies. In addition, the term "information" is a very broad one, and is capable of covering *e.g.* communications and communications data that a foreign intelligence agency has obtained.

47. By s. 19(2) of the CTA:

> "*Information obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that service in connection with the exercise of any of its other functions*."

It is thus clear that *e.g.* information that is obtained by the Security Service for national security purposes (by reference to s. 1(2) of the SSA) can subsequently be used by the Security Service to support the activities of the police in the prevention and detection of serious crime (pursuant to s. 1(4) of the SSA).

The HRA

48. Art. 8 of the ECHR is a "Convention right" for the purposes of the HRA: s. 1(1) of the HRA. Art. 8, set out in Sch. 1 to the HRA, provides as follows:

> "*(1) Everyone has the right to respect for his private and family life, his home and his correspondence.*
> *(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevent of disorder or crime, for the protection of health and morals, or for the protection of the rights and freedoms of others*."

49. By s. 6(1):

> "*It is unlawful for a public authority to act in a way which is incompatible with a Convention right*."

50. Each of the Intelligence Services is a public authority for this purpose. Thus, when undertaking any activity that interferes with Art. 8 rights, the Intelligence Services must (among other things) act proportionately.

51. S. 7(1) of the HRA provides in relevant part:

> "*A person who claims that a public authority has acted (or proposes to act) in a way*

---

[17] By s. 19(5), information obtained by GCHQ for the purposes of any of its functions "*may be disclosed by it - (a) for the purpose of the proper discharge of its functions, or (b) for the purpose of any criminal proceedings*."

which is made unlawful by section 6(1) may –

(a) bring proceedings against the authority under this Act in the appropriate court or tribunal ...."

The DPA

52. Each of the Intelligence Services is a data controller (as defined in s. 1(1) of the DPA) in relation to all the personal data (as defined in s. 1(1) of the DPA) that it holds. Insofar as the obtaining of an item of information by any of the Intelligence Services amounts to an interference with Art. 8 rights, that item of information will in general amount to personal data.

53. As a data controller, each of the Intelligence Services is in general required by s. 4(4) of the DPA to comply with the data protection principles in Part I of Sch. 1 to the DPA. That obligation is subject to ss. 27(1) and 28(1) of the DPA, which exempt personal data from (among other things) the data protection principles if the exemption "*is required for the purpose of safeguarding national security*". By s. 28(2) of the DPA, a Minister may certify that exemption from the data protection principles is so required. Copies of the ministerial certificates for each of the Intelligence Services are available on request. Those certificates certify that personal data that are processed in performance of the Intelligence Services' functions are exempt from the first, second and eighth data protection principles (and are also exempt in part from the sixth data protection principle). Thus the certificates do <u>not</u> exempt the Intelligence Services from their obligation to comply with the fifth and seventh data protection principles, which provide:

"*5.Personal data processed*[18] *for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. …*

7.
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."[19]

54. Accordingly, when the Intelligence Services obtain any information from a foreign intelligence agency that amounts to personal data, they are obliged:

54.1 not to keep that data for longer than is necessary having regard to the purposes for which they have been obtained and are being retained / used; and

54.2 to take appropriate technical and organisational measures to guard against unauthorised or unlawful processing of the data in question and against accidental loss of the data in question. (See also, in this

[18] The term "processing" is broadly defined in s. 1(1) of the DPA to include (among other things), obtaining, recording and using.
[19] The content of the obligation imposed by the seventh data protection principle is further elaborated in §§9-12 of Part II of Sch. 1 to the DPA.

regard, §56 below).

The OSA

55. A member of the Intelligence Services commits an offence if "*without lawful authority he discloses any information, document or other article relating to security or intelligence which is or has been in his possession by virtue of his position as a member of any of those services*": s. 1(1) of the OSA. A disclosure is made with lawful authority if, and only if, it is made in accordance with the member's official duty (s. 7(1) of the OSA). Thus, a disclosure of information by a member of the Intelligence Services that is *e.g.* in breach of the relevant "arrangements" (under, as the case may be, s. 2(2)(a) of the SSA, s. 2(2)(a) of the ISA or s. 4(2)(a) of the ISA) will amount to a criminal office. Conviction may lead to an imprisonment for a term not exceeding two years and/or a fine (s. 10(1) of the OSA).

56. Further, a member of the Intelligence Services commits an offence if he fails to take such care, to prevent the unauthorised disclosure of any document or other article relating to security or intelligence which is in his possession by virtue of his position as a member of any of those services, as a person in his position may reasonably be expected to take. See s. 8(1) of the OSA, as read with s. 1(1). Conviction may lead to an imprisonment for a term not exceeding three months and/or a fine (s. 10(2) of the OSA).

RIPA

57. In general,[20] the Intelligence Services are not required to seek authorisation under RIPA in order to obtain communications or communications data from foreign intelligence agencies. However, this does not mean that RIPA is of no relevance in the present context.

58. In particular, not least given the safeguards and oversight mechanisms that Parliament saw fit to impose in the case of interception pursuant to a RIPA interception warrant (see §§102-178 below), and in the light of the well-established *Padfield* principle,[21] it is accepted that it would as a matter of domestic public law be unlawful for any of the Intelligence Services to deliberately circumvent those safeguards and mechanisms (and attempt to avoid the need to apply for an interception warrant under RIPA) by asking a foreign intelligence agency to intercept certain specified communications and disclose them. That is not to say that there will not be circumstances where there are legitimate reasons to ask a foreign intelligence agency to intercept particular communications, for example, where it is not technically feasible for the Intelligence Services themselves to undertake the interception in question.

---

[20] The position is somewhat different as regards requests for assistance under the Convention on Mutual Assistance in Criminal Matters between Member States of the European Union, 2000/C197/01. See ss. 1(4) and 5(1)(b) of RIPA, as read with the Regulation of Investigatory Powers (Designation of an International Agreement) Order 2004, SI 2004/158.

[21] *Padfield v. Minister of Agriculture, Fisheries and Food* [1968] AC 997, *per* Lord Reid at 1030B-D.

59. Similarly, it would as a matter of basic public law be unlawful for any of the Intelligence Services to deliberately circumvent the provisions in Chapter II of Part I of RIPA or any other domestic legislation governing the acquisition of communications data by asking a foreign intelligence agency to obtain specified communications data and disclose them. Again, that is not to say that there will not be circumstances where there are legitimate reasons to ask a foreign intelligence agency to obtain particular communications data, *e.g.* for reasons of technical feasibility.

Oversight mechanisms in the Intelligence Sharing regime

60. There are two principal oversight mechanisms in the Intelligence Sharing regime:

    60.1 The ISC; and

    60.2 The Tribunal.

The ISC

61. SIS and GCHQ are responsible to the Foreign Secretary,[22] who in turn is responsible to Parliament. Similarly, the Security Service is responsible to the Home Secretary, who in turn is responsible to Parliament. In addition, the ISC plays an important part in overseeing the 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.

62. The ISC was established by s. 10 of the ISA. As from 25 June 2013, the statutory framework for the ISC is set out in ss. 1-4 of and Sch. 1 to the Justice and Security Act 2013 ("the JSA").

63. The ISC consists of nine members, drawn from both the House of Commons and the House of Lords. Each member is appointed by the House of Parliament from which the member is to be drawn (they must also have been nominated for membership by the Prime Minister, following consultation with the leader of the opposition). No member can be a Minister of the Crown. The Chair of the ISC is chosen by its members. See s. 1 of the JSA.

64. The executive branch of Government has no power to remove a member of the ISC: a member of the ISC will only vacate office if he ceases to be a member of the relevant House of Parliament, becomes a Minister of the Crown or a resolution for his removal is passed by the relevant House of Parliament. See §1(2) of Sch. 1 to the JSA.

[22] The Chief of the Intelligence Service and the Director of GCHQ must each make an annual report on, respectively, the work of SIS and GCHQ to the Prime Minister and the Secretary of State (see ss. 2(4) and 4(4) of the ISA). An analogous duty is imposed on the Director-General of the Security Service (see s. 2(4) of the SSA).

65. The current chair is Sir Malcolm Rifkind MP. He is a former Secretary of State for Defence and a former Secretary of State for Foreign and Commonwealth Affairs.

66. The ISC may examine the expenditure, administration, policy and operations of each of the Intelligence Services: s. 2(1). Subject to certain limited exceptions, the Government (including each of the Intelligence Services) must make available to the ISC information that it requests in the exercise of its functions. See §§4-5 of Sch. 1 to the JSA. The ISC operates within the "ring of secrecy" which is protected by the OSA. It may therefore consider classified information, and in practice takes oral evidence from the Foreign and Home Secretaries, the Director-General of the Security Service, the Chief of SIS and the Director of GCHQ, and their staff. The ISC meets at least weekly whilst Parliament is sitting. Following the extension to its statutory remit as a result of the JSA, the ISC is further developing its investigative capacity by appointing additional investigators.

67. The ISC must make an annual report to Parliament on the discharge of its functions (s. 3(1) of the JSA), and may make such other reports to Parliament as it considers appropriate (s. 3(2) of the JSA). Such reports must be laid before Parliament (see s. 3(6)). They are as necessary redacted on security grounds (see ss. 3(3)-(5)), although the ISC may report redacted matters to the Prime Minister (s. 3(7)). The Government lays before Parliament any response to the reports that the ISC makes.

68. The ISC sets its own work programme: it may issue reports more frequently than annually and has in practice done so for the purposes of addressing specific issues relating to the work of the Intelligence Services.

The Tribunal

69. The Tribunal was established by s. 65(1) of RIPA. Members of the Tribunal must either hold or have held high judicial office, or be a qualified lawyer of at least 7 years' standing (§1(1) of Sch. 3 to RIPA). The President of the Tribunal must hold or have held high judicial office (§2(2) of Sch. 3 to RIPA).

70. The Tribunal's jurisdiction is broad. As regards the Intelligence Sharing regime, the following aspects of the Tribunal's jurisdiction are of particular relevance:

    70.1 The Tribunal has exclusive jurisdiction to consider claims under s. 7(1)(a) of the HRA brought against any of the Intelligence Services or any other person in respect of any conduct, or proposed conduct, by or on behalf of any of the Intelligence Services (ss. 65(2)(a), 65(3)(a) and 65(3)(b) of RIPA).

    70.2 The Tribunal may consider and determine any complaints by a person who is aggrieved by any conduct by or on behalf of any of the Intelligence Services which he believes to have taken place in relation to him, to any of his property, to any communications sent by or to him, or intended for him, or to his use of any telecommunications

service or system (ss. 65(2)(b), 65(4) and 65(5)(a) of RIPA).

71. Complaints of the latter sort must be investigated and then determined "by applying the same principles as would be applied by a court on an application for judicial review" (s. 67(3)).

72. Thus the Tribunal has jurisdiction to consider any claim against any of the Intelligence Services that it has obtained information from a foreign intelligence agency in breach of the ECHR or has disclosed information to a foreign intelligence agency in breach of the ECHR. Further, the Tribunal can entertain any other public law challenge to any such alleged obtaining or disclosure of information.

73. Any person, regardless of nationality, may bring a claim in the Tribunal. Further, a claimant does not need to be able to adduce cogent evidence that some step has in fact been taken by the Intelligence Services in relation to him before the Tribunal will investigate.[23] As a result, the Tribunal is perhaps one of the most far-reaching system of judicial oversight over intelligence matters in the world.

74. Pursuant to s. 68(2), the Tribunal has a broad power to require a relevant Commissioner (as defined in s. 68(8)) to provide it with assistance. Thus, in the case of a claim of the type identified in §72 above, the Tribunal may require the Intelligence Services Commissioner (see ss. 59-60 of RIPA) to provide it with assistance.

75. S. 68(6) imposes a broad duty of disclosure to the Tribunal on, among others, every person holding office under the Crown.

76. Subject to any provision in its rules, the Tribunal may - at the conclusion of a claim - make any such award of compensation or other order as it thinks fit, including, but not limited to, an order requiring the destruction of any records of information which are held by any public authority in relation to any person. See s. 67(7).

The issues of pure law suitable for determination at a Legal Issues Hearing

77. It is submitted that the following issues of pure law relating to Prism appear from the Grounds advanced by Privacy International and Liberty:

Issue (i)

Does the Intelligence Sharing regime satisfy the requirement in Art. 8(2) that any interference be "in accordance with the law"?

[23] The Tribunal may refuse to entertain a claim that is frivolous or vexatious (see s. 67(4)), but in practice it has not done so merely on the basis that the claimant is himself unable to adduce evidence to establish *e.g.* that the Intelligence Services have taken some step in relation to him. There is also a 1 year limitation period (subject to extension where that is "equitable"): see s. 67(5) of RIPA and s. 7(5) of the HRA.

Issue (ii)

Does the Intelligence Sharing regime ensure that the obtaining, retention and disclosure of information by the Intelligence Services pursues one or more legitimate aims for the purposes of Art. 8(2)?

78. In addition, the Tribunal can in principle investigate in closed session:

78.1 whether in fact any of the Claimants' communications and communications data were obtained by any of the Intelligence Services via Prism;

78.2 if they were, whether those communications / data were retained, disclosed or used in any other way; and

78.3 whether, in the light of all the relevant facts and circumstances, and irrespective of whether the overall Intelligence Sharing regime is proportionate for the purposes of Art. 8(2), any obtaining, retention, disclosure or other use of those communications / data that in fact took place was a proportionate interference with the Claimants' Art. 8 rights.

79. It appears that the Claimants do not specifically invite the Tribunal to investigate the matters set out in §78 above, and correspondence from them dated 1 November 2013 suggests that they may in the event specifically request the Tribunal not to do so. Subject to an unequivocal request of this type, the Respondents would respectfully invite the Tribunal to investigate the matters set out in §78 above, as part of its investigative functions, and insofar as it is possible to do so given the limited information provided by the Claimants as to the "factors" which could be used in any searches by the Intelligence Services.

Issue (i): Does the Intelligence Sharing regime satisfy the requirement in Art. 8(2) that any interference be "in accordance with the law"?

80. The expression "in accordance with the law" requires:

> "*... firstly, that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him, and compatible with the rule of law ...*" (*Weber*, at §84.)

81. The Intelligence Sharing regime is "accessible" and has a basis in domestic law, in that it consists of provisions in primary legislation. Privacy International's argument that there is no relevant legal regime that regulates the circumstances in which and the conditions on which the Intelligence Services may obtain information from the US authorities[24] is untenable given §§36-76 above.

[24] See *e.g.* §43 of Privacy International's Statement of Grounds.

82. Further, it appears to be common ground (see §71(6) of Liberty's Grounds of Claim) that the intelligence activities / operations of the foreign State which is sharing intelligence with the Intelligence Services do not themselves need somehow to satisfy the Art. 8 "in accordance with the law" requirement. Moreover, and for the avoidance of doubt, it is no part of the Respondent's case that the US legal framework somehow itself renders any interferences with Art. 8(1) rights for which the Intelligence Services are responsible "in accordance with the law" for Art. 8(2) purposes (compare §73 of Liberty's Grounds of Claim). The adequacy of the relevant US law is a matter for the US Courts and not (it is respectfully submitted) the Tribunal.

83. In relation to 'foreseeability' in this context, the essential test, as recognised in §68 of *Malone*, is whether the law indicates the scope of any discretion and the manner of its exercise with sufficient clarity "***to give the individual adequate protection against arbitrary interference***". As the Grand Chamber recently confirmed in the eavesdropping case of *Bykov v. Russia*, appl. no. 4378/02, judgment of 21 January 2009, this test remains the guiding principle when determining the foreseeability of intelligence-gathering powers (see §78).[25]

84. Moreover, the ECtHR has consistently recognised that the foreseeability requirement cannot mean that an individual should be enabled to foresee when the authorities are likely to resort to secret measures so that he can adapt his conduct accordingly: *Malone v. UK* (1984) 7 EHRR14, at §67; *Leander v. Sweden* (1987) 9 EHRR 433, at §51; and *Weber*, at §93.

85. In the Strasbourg cases, concerning the exercise of domestic powers of interception, such as *Weber* and *Liberty v. UK* (2009) 48 EHRR 1, the ECtHR has built on the test in §68 of *Malone* by developing a specific list of "minimum safeguards" that have to be set out in the domestic interception regime in order to satisfy the "foreseeability" requirement:

> "*the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed ...*" (*Weber*, at §95).

86. However, it is important to appreciate that cases such as *Weber* and *Liberty* concern interception **by the respondent State**. The Claimants do not cite any Art. 8 case that concerns a complaint that the intelligence agencies of the respondent State had secretly obtained information from **another** State (whether in the form of communications that that other State had itself intercepted, or otherwise). Indeed, so far as the Respondents are aware, the

[25]The "necessity" requirement also calls for adequate and effective safeguards against abuse. But the Tribunal is sufficient for this purpose: §59 of *Rotaru v. Romania* (2000) 8 BHRC 449 ("*effective supervision ... should normally be carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure* ..."). *A fortiori*, the combination of the Tribunal and the ISC satisfies this aspect of the "necessity" requirement.

application of Art. 8 to cases of this latter type has never been considered in Strasbourg or in the domestic courts.

87. It is submitted that, not merely is there no authority indicating that the specific principles that have been developed in cases involving interception by the respondent State are to be applied in the distinct factual context where the intelligence agencies of the respondent State have merely obtained information from a foreign State, but there are also good reasons of principle why that should not be so.

88. **First**, the ECtHR has expressly recognised that the "rather strict standards" developed in the recent Strasbourg intercept cases do not necessarily apply in other intelligence-gathering contexts: *Uzun v. Germany* (2011) 53 EHRR 24, at §66. See also *McE v. Prison Service of Northern Ireland* [2009] 1 AC 908, *per* Lord Carswell at §85.

89. **Secondly**, and as a matter of principle, there is no good reason to single out communications / communications data from amongst all the types of information that might in principle be obtained from a foreign intelligence agency. The Claimants argument proves too much. If the principles in the recent Strasbourg intercept cases apply to the obtaining of communications / communications data from a foreign intelligence agency, and if the Intelligence Sharing regime does not satisfy those principles, then it is difficult to see how the Intelligence Services could lawfully obtain <u>any</u> information from a foreign intelligence agency (at least insofar as it is private and personal). But that would be a remarkable conclusion, not least given that intelligence sharing is (and has for many years been) vital to the effective operation of the Intelligence Services.

90. **Thirdly**, it would plainly not be feasible for a domestic legal regime to (i) set out in detail <u>all</u> the various types of information that may be obtained from each of the various foreign States with which the State at issue might share intelligence, (ii) define the tests to be applied when determining whether to obtain each such type of information and the limits on access and (iii) set out the handling, etc. requirements and the uses to which all such types of information may be put.[26] Nor is there any suggestion that the ECtHR has ever suggested that this is necessary (and see §96 of *S and Marper v. UK* (2009) 48 EHRR 50: domestic legislation "cannot in any case provide for every eventuality").

91. There is a final point on the approach to be adopted by domestic courts and tribunals. The challenges here raise issues as to the compatibility of the domestic legal regimes with Art. 8 in a thoroughly important and sensitive context. In taking account of the ECtHR jurisprudence (s. 2 of the HRA), the Tribunal should go no further than is required by clear and constant

[26] Whilst guidance has been promulgated on the detention and interviewing of detainees overseas (see the July 2010 guidance, "*Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees*"), this guidance is not intended to make the activities of UK public authorities in this regard more "foreseeable" for Art. 8 purposes.

jurisprudence of the ECtHR. To do otherwise would be contrary to the constitutional settlement in the HRA, and at a practical level would in effect deprive the Government of the possibility of inviting the ECtHR to opine on the issues arising: see *e.g. R (Ullah) v. Special Adjudicator* [2004] 2 AC 323, *per* Lord Bingham at §20; and *R (Al Skeini) v. Secretary of State for Defence* [2008] 1 AC 153, *per* Lord Brown at §106. In the present context, there is (for the reasons given) no such clear and constant jurisprudence; and there are good reasons not to extend principles developed in the context of domestic controls over domestic intercept more broadly into the territory of obtaining information from foreign intelligence agencies.

92. Thus, the test to be applied is whether the Intelligence Sharing regime indicates the scope of any discretion and the manner of its exercise with sufficient clarity "to give the individual adequate protection against arbitrary interference" (*Malone*, at §68).

93. It is submitted that the regime plainly satisfies this test:

93.1 Given §§38-50 above, the Intelligence Sharing regime is sufficiently clear as regards the circumstances in which each of the Intelligence Services can **obtain** information (including in the form of communications) from foreign intelligence agencies. See *Esbester v. UK* (1994) 18 EHRR CD72, *Hewitt v. UK* (1992) 14 EHRR 657 and *Redgrave v. UK*, Appl. No. 20271/92, Commission decision of 1 September 1993.

93.2 The Intelligence Sharing regime is similarly sufficiently clear as regards the subsequent **handling, use and possible onward disclosure** of information so obtained. See §§38-54 above.

93.3 These conclusions apply *a fortiori* to communications data, given that the covert acquisition of such data is less intrusive in Art. 8 terms than the covert acquisition of the content of communications. See *Malone* at §84.

94. In the alternative, if some version of the list of "safeguards" in *e.g.* §95 of *Weber* applies to the obtaining of information from a foreign intelligence agency, the present regime satisfies the requirements for such "safeguards", insofar as it is feasible to do so. See §§93.1-93.3 above.

Issue (ii): Does the Intelligence Sharing regime ensure that the obtaining, retention and disclosure of information by the Intelligence Services pursues one or more legitimate aims for the purposes of Art. 8(2)?

95. S. 2(2) of the SSA and ss. 2(2) and 4(2) of the ISA ensure that, for the purposes of Art. 8(2), information (including communications and communications data) can only be obtained by the Intelligence Services from foreign intelligence agencies for legitimate aims. Further, those same provisions ensure that any disclosure of such information by the Intelligence Services must equally pursue one or more legitimate aims.

96. Insofar as the retention of information by the Intelligence Services amounts to

a separate Art. 8 interference, then s. 6 of the HRA ensures that the Intelligence Services cannot lawfully retain information otherwise than for one or more legitimate aims. (The same result follows as a matter of domestic law given the limited functions of the Intelligence Services, as set out in the SSA and the ISA.)

IV. THE ALLEGED "TEMPORA" INTERCEPTION OPERATION

The facts

97. Ground 2 in Privacy International's Statement of Grounds and the Second and the Third Grounds in Liberty's Grounds of Claim concern an alleged GCHQ intelligence operation (called, by Privacy International and Liberty, "Tempora"), to which reference has been made in various news reports (including in *The Guardian* newspaper on 21 June 2013).

98. Privacy International claims that this alleged operation has been taking place under interception warrants issued pursuant to s. 8(4) of RIPA (Statement of Grounds, §49). For convenience, such warrants will be referred to below as "s. 8(4) warrants", and the legal regime which governs interception under such warrants will be referred to as "the s. 8(4) regime". §78 of Liberty's Grounds of Claim states that the alleged "Tempora" operation "appears" to be based on the s. 8(4) regime, but also raises the possibility that this alleged operation may involve "the interception of stored communications without warrant" under s. 1(5)(c) of RIPA[27] and/or "one or more authorisations to obtain communications data" under s. 22(5) of RIPA.

99. For all the reasons set out above, the Respondents neither confirm nor deny the existence of the alleged "Tempora" operation; nor any of the factual claims relating to this alleged operation in Privacy International's Statement of Grounds and Liberty's Grounds of Claim. Further, and for the avoidance of doubt, the Respondents neither confirm nor deny (i) whether any of the Claimants' communications were intercepted under the s. 8(4) regime, or, if they were intercepted, (ii) whether any of those communications so intercepted were read, looked at or listened to by any person. (For the purposes of the s. 8(4) regime there is a significant distinction between the interception of a communication in and of itself and the examination of a communication that has been so intercepted: see §§126-131 below).

100. The Respondents nevertheless accept that the Claimants may challenge the

[27] Liberty argues, in effect, that if the alleged "Tempora" operation relies (to any degree) on s. 1(5)(c) of RIPA then this would be unlawful because it would fall outside what Liberty characterises as the "narrow" scope of s. 1(5)(c) (as a matter, it seems, of domestic law) and/or would breach Art. 8(2) (§§88 and 89(1) of the Grounds of Claim). Liberty's arguments in this regard suffer from the fatal flaw that they fail to recognise that s. 1(5)(c) is not a free-standing provision. Section 1(5)(c) refers to, and - in its operation - depends upon, other statutory powers for the purpose of obtaining information or of taking possession of any document or other property. This Response therefore does not further address Liberty's arguments under s. 1(5)(c).

general Art. 8-compatibility of the s. 8(4) regime on the basis that their communications might in principle have been intercepted[28] and that at least some of those intercepted communications might in principle have been "read, looked at or listened to" by a person or persons. See *e.g.* §78 of *Weber*.

101. However, for the reason given in §35 above, Liberty cannot claim to be victims of any Art. 10 interferences (compare §98(1) of Liberty's Grounds of Claim). Privacy International (rightly) does not bring an Art. 10 claim in relation to the alleged "Tempora" operation.

The s. 8(4) regime

102. The s. 8(4) regime is principally contained in RIPA and the Interception Code of Practice, as elucidated by the Tribunal in the 9 December 2004 ruling in IPT/01/77 ("the s. 8(4) Ruling").[29] The s. 8(4) regime also incorporates aspects of the Information Sharing regime addressed above.

103. Section 71 of RIPA imposes a duty on the Secretary of State to issue, following appropriate consultation, one or more codes of practice relating to the exercise and performance of the powers and duties conferred or imposed by or under Part I of RIPA (which includes ss. 1-19). Any person exercising or performing any power or duty under ss. 1-19 must have regard to any relevant provisions of every code of practice for the time being in force: s. 72(1). Further, where the provision of a code of practice appears to the Tribunal, a court or any other tribunal to be relevant to any question arising in the proceedings, in relation to a time when it was in force, that provision of the code must be taken account in determining that question. A similar duty is imposed on the Commissioner: see s. 72(4) of RIPA. The Code of Practice can be taken into account in assessing "foreseeability" for the purposes of Art. 8(2): *Kennedy*, at §157.

104. A code of practice ("the Code") was issued in relation to the interception of communications on 1 July 2002.[30]

The interception of communications under RIPA

105. Section 2 of RIPA provides a detailed definition of the concept of "interception".[31]

105.1 By s. 2(2), interception occurs if (among other things) a person "modifies or interferes with" a telecommunications system so as to

[28] The Respondents accept that the interception of a communication under a s. 8(4) warrant may be regarded as giving rise to a technical interference with the Art. 8 rights of the parties to the communication even if that communication is not and/or cannot be read, looked at or listened to by any person.

[29] A judicial decision of this type can be taken into account in assessing "foreseeability" for the purposes of Art. 8(2): *Uzun v. Germany* (2011) 53 EHRR 24, at §62.

[30] Not 2007, as claimed by Liberty (see §81 of the Grounds of Claim).

[31] Strictly speaking, the concept of intercepting a communication in the course of its transmission by means of a telecommunications system. The distinction is not, however, relevant for present purposes.

make "available" the content of a communication which is being transmitted on that system "to a person other than the sender or intended recipient of the communication". By s. 2(1), the term "telecommunications system" means:

> "*... any system (including the apparatus comprised in it) which exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy.*"

105.2 By s. 2(6), the "modification" of a telecommunications system includes "*the attachment of any apparatus to, or other modification of or interference with ... any part of the system*".

105.3 Significantly, by s. 2(8):

> "*For the purposes of this section the cases in which any contents of a communication are to be taken to be made available to a person while being transmitted shall include any case in which any of the contents of the communication, while being transmitted, are diverted or recorded so as to be available to a person subsequently.*"

106. In other words, "interception" can merely comprise the obtaining and recording of a communication (as it is being transmitted) so as to make it "available" subsequently to be read, looked at or listened by a person. No-one in fact needs to have actually read, looked at or listened to the communication for interception to occur: the intercepted communication may simply be stored on a computer for a period, and then deleted, without ever being read, etc. by anyone.

107. Under s. 1(1) of RIPA it is an offence, punishable by a term of imprisonment of up to two years and a fine,[32] for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of a public telecommunications system. The Commissioner (see §§161-174 below) also has power to serve a monetary penalty notice (of up to £50,000) on a person who has intercepted a communication without lawful authority (in circumstances which do not amount to an offence under s. 1(1)), and who was not making an attempt to act in accordance with a warrant (see s. 1(1A)).

108. Conduct has lawful authority for the purposes of s. 1 if it takes place in accordance with a warrant under s. 5 of RIPA ("an interception warrant"): s. 1(5)(b).[33] A s. 8(4) warrant is an interception warrant for this purpose.

---

[32] See s. 1(7).

[33] For the purposes of §98 above, it may also be noted that conduct has lawful authority for the purposes of s. 1 if "*it is in exercise, in relation to any stored communication, of any statutory power that is exercised (apart from this section) for the purpose of obtaining information or of taking possession of any document or other property*" (s. 1(5)(c)).

The issuing of interception warrants

109. Interception warrants are issued by the Secretary of State under s. 5(1) of RIPA. Generally, such warrants must be issued personally by the Secretary of State: s. 7 of RIPA.

110. An application must be made before an interception warrant can be issued: s. 6(1) of RIPA. Such an application may only be made by or on behalf of one of the persons listed in s. 6(2) of RIPA (which list includes the Director-General of the Security Service, the Chief of SIS and the Director of GCHQ). The application must contain all the detailed matters set out in §5.2 of the Code. This ensures that the Secretary of State has the information he needs properly to determine, under the statutory tests, whether to issue an interception warrant.

111. The Commissioner has recognised that the Secretaries of State in question take their responsibilities "*very seriously*" (see the Foreword of the Commissioner's 2012 Annual Report; see also §§6.6.1 and 6.6.2).

112. By s. 5(2) of RIPA, the Secretary of State may not issue an interception warrant unless he believes:

> "*(a) that the warrant is necessary on grounds falling within subsection (3); and*
> *(b) that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct*."

113. When considering whether the requirements of s. 5(2) are satisfied, the Secretary of State must take into account "*whether the information which it is thought necessary to obtain under the warrant could reasonably be obtained by other means*": see s. 5(4) of RIPA.

114. A warrant is necessary on grounds falling within s. 5(3) only if it is necessary (a) in the interests of national security, (b) for the purpose of preventing or detecting[34] serious crime[35] or (c) for the purpose of safeguarding the economic well-being of the United Kingdom. A limitation on purpose (c) is provided by s. 5(5) of RIPA:

> "*A warrant shall not be considered necessary [for the purpose of safeguarding the economic well-being of the United Kingdom] unless the information which it is thought necessary to obtain is information relating to the acts or intentions of persons outside the British Islands*[36]."

115. As regards the s. 8(4) regime, §5.4 of the Code further narrows purpose (c): the Secretary of State must consider whether the economic well-being of the United Kingdom which is to be safeguarded is, on the facts of the case, directly related to national security, and the Secretary of State cannot issue a

[34] The terms "preventing" and "detecting" are defined in s. 81(5) of RIPA.
[35] The term "serious crime" is defined in ss. 81(2)(b) and 81(3) of RIPA.
[36] Defined by s. 5 of and Sch. 1 to the Interpretation Act 1978 to mean the United Kingdom, the Channel Islands and the Isle of Man.

warrant on s. 5(3)(c) grounds unless such a "direct link" has been established.

116. All warrant applications under the s. 8(4) regime must be kept so that they can be scrutinised by the Commissioner: §5.17 of the Code.

Section 8(4) warrants

117. The contents of interception warrants are dealt with under s. 8 of RIPA. Provision is made for two types of warrant. The type of warrant of relevance in the present case - a s. 8(4) warrant - is provided for in s. 8(4)-(6):

> *"(4) Subsections (1) and (2)[37] shall not apply to an interception warrant if-*
> *(a) the description of communications to which the warrant relates confines the conduct authorised or required by the warrant to conduct falling within subsection (5); and*
> *(b) at the time of the issue of the warrant, a certificate applicable to the warrant has been issued by the Secretary of State certifying-*
> *(i) the descriptions of intercepted material[38] the examination of which he considers necessary; and*
> *(ii) that he considers the examination of material of those descriptions necessary as mentioned in section 5(3)(a), (b) or (c).*
> *(5) Conduct falls within this subsection if it consists in-*
> *(a) the interception of external communications in the course of their transmission by means of a telecommunication system; and*
> *(b) any conduct authorised in relation to any such interception by section 5(6).*
> *(6) A certificate for the purposes of subsection (4) shall not be issued except under the hand of the Secretary of State."*

118. The term "communication" is defined broadly in s. 81(1) of RIPA to include (among other things) "*anything comprising speech, music, sounds, visual images or data of any description*". The term "external communication" is defined in s. 20 to mean "a communication sent or received outside the British islands". In addition, §5.1 of the Code provides:

> "[*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*."

119. By s. 5(1), a warrant may authorise or require:

> *"... the person to whom it is addressed, by any such conduct as may be described in the warrant, to secure any one or more of the following –*
> *(a) the interception in the course of their transmission by means of a postal service or telecommunication system of the communications described in the warrant ..."*

---

[37] See §125 below.

[38] Defined in s. 20 to mean, in relation to an interception warrant, "the contents of any communications intercepted by an interception to which the warrant relates".

120. Further, s. 5(6) provides in relevant part:

> "*The conduct authorised by an interception warrant shall be taken to include –*
> *(a) all such conduct (including the interception of communications not identified by the warrant) as it is necessary to undertake in order to do what is expressly authorised or required by the warrant;*
> *(b) conduct for obtaining related communications data*[39]*;...*"

121. The reference in s. 5(6)(a) to "communications" as opposed to "external communications" is to be noted. In particular, s. 5(6)(a) makes clear that the conduct authorised by a s. 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.

122. The s. 8(4) regime does not impose any express limit on the number of external communications which may fall within "*the description of communications to which the warrant relates*" in s. 8(4)(a). Thus, as the Tribunal observed at §9 of the s. 8(4) Ruling, a s. 8(4) warrant:

> "*... can and may result, provided that the requirements of s8(4) and (5) are satisfied, in the interception of all communications between the United Kingdom and an identified city or country.*" (Emphasis added.)

123. Similarly, the s. 8(4) regime does not seek to limit the type of communications at issue for the purposes of s. 8(5)(a), save for the requirement that they be "external". Thus the broad definition of "communication" in s. 81 applies and, in principle, anything that falls within that definition may fall within s.8(5)(a) insofar as it is "external".

124. Like all applications for s. 8(4) warrants, the warrants themselves (and their accompanying certificates) must be kept so as to be available to be scrutinised by the Commissioner: see §5.17 of the Code.

125. The other type of interception warrant ("a s. 8(1) warrant") should also be noted. A s. 8(1) warrant conforms to the requirements of s. 8(1)-(3) of RIPA:

> "*(1) An interception warrant must name or describe either-*
> *(a) one person as the interception subject; or*
> *(b) a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place.*
> *(2) The provisions of an interception warrant describing communications the interception of which is authorised or required by the warrant must comprise one or more schedules setting out the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying the communications that may be or are to be intercepted.*

[39] "Related communications data", in relation to a communication intercepted in the course of transmission by means of a telecommunication system, is defined to be so much of any communications data as (a) is obtained by, or in connection with, the interception; and (b) relates to the communication. See s. 20 of RIPA.

(3) Any factor or combination of factors set out in accordance with subsection (2) must be one that identifies communications which are likely to be or to include-

(a) communications from, or intended for, the person named or described in the warrant in accordance with subsection (1); or

(b) communications originating on, or intended for transmission to, the premises so named or described."[40]

Processing the intercepted communications to obtain communications that can be read, looked at or listened to

126. By s. 15(1)(b) of RIPA, the Secretary of State is under a duty to ensure, in relation to s. 8(4) warrants, that such arrangements are in force as he considers necessary for securing that the requirements of s. 16 are satisfied.

127. Section 16(1) imposes the requirement that:

"*…the intercepted material is read, looked at or listened to by the persons to whom it becomes available by virtue of the warrant to the extent only that it-*

(a) has been certified as material the examination of which is necessary as mentioned in section 5(3)(a), (b) or (c); and

(b) falls within subsection (2)."

128. Section 16(2) provides in relevant part:

"*…intercepted material falls within this subsection so far only as it is selected to be read, looked at or listened to otherwise than according to a factor which-*

(a) is referable to an individual who is known to be for the time being in the British Islands; and

(b) has as its purpose, or one of its purposes, the identification of material contained in communications sent by him, or intended for him."

129. Section 16(2) is subject to ss. 16(3) and 16(4), which provide for strictly limited circumstances in which it is permissible to select intercepted material by reference to factors which satisfy ss. 16(2)(a) and 16(2)(b).

130. In addition, pursuant to s. 6(1) of the HRA, the selection of any particular intercepted material to be read, looked at or listened to must always be proportionate, having regard to the particular circumstances, for Art. 8(2) purposes.

131. Thus, the s. 8(4) regime envisages the following:

131.1 A volume of intercepted material will be generated by the act of interception pursuant to a s. 8(4) warrant. The volume may <u>in principle</u> be substantial (see §9 of the s. 8(4) Ruling, as set out in §122 above; and see also the reference to a "large quantity of as yet unexamined material" in §34 of the s. 8(4) Ruling). Further, the

[40] Liberty is wrong to claim (in §28 of its Statement of Grounds) that s. 8(1) and 8(2) of RIPA "do not apply" to external communications. <u>In principle</u>, the person or set of premises to which reference is made in s. 8(1) need <u>not</u> be within the British Islands.

intercepted material may be recorded so as to be available for subsequent examination (see s. 2(8) of RIPA, and §§105.3-106 above).

131.2 Pursuant to the s. 16 arrangements, a smaller volume of intercepted material is then selected to be read, looked at or listened to by persons. The intercepted material so selected must be certified (in the Secretary of State's certificate) as material the examination of which is necessary as mentioned in s. 5(3)(a), (b) or (c) of RIPA (*i.e.* in interests of national security, for the purpose of preventing or detecting serious crime or for the purpose of safeguarding the economic well-being of the United Kingdom). In other words, the certificate regulates the examination of the intercepted material (see §5.2 of the Code). In addition, any individual selection of intercepted material must be proportionate in the particular circumstances (given s. 6(1) of the HRA). Further, provision is made in s. 16 of RIPA to limit the extent to which intercepted material can be selected by reference to "factors" that in essence would select communications to or from an individual who is known to be (at the time) in the British Islands.

131.3 Insofar as the intercepted material may not be proportionately selected to be read, looked at or listened to in accordance with the certificate and pursuant to s. 16 of RIPA and s. 6(1) of the HRA, then it cannot be read, looked at or listened to by anyone.

132. There is thus considerable importance in the distinction between the act of interception in and of itself; and a person actually reading, looking at or listening to intercepted material.

133. Records must be kept of the s. 16 arrangements, and they must be made available to the Commissioner (§§5.17 and 6.1 of the Code), who is required to keep them under review (see s. 57(2)(d)(i) of RIPA). Any breach of the arrangements must be reported to the Commissioner (§6.1 of the Code). Further, if the Commissioner considers that the arrangements have proved inadequate in any relevant respect he must report this to the Prime Minister (see s. 58(3)).

134. The Commissioner's advice and approval was sought and given in respect of the documents constituting the s. 16 arrangements either before or shortly after 2 October 2000 (when RIPA came into force): §15 of the Commissioner's Annual Report for 2000. In practice, the advice of the Commissioner is sought when any substantive change is proposed to the arrangements.

The duration, cancellation, renewal and modification of warrants and certificates under RIPA

135. A s. 8(4) warrant ceases to have effect at the end of the "relevant period", unless it is renewed by an instrument under the hand of the Secretary of State: s. 9(1) of RIPA. The "relevant period" for a s. 8(4) warrant is, depending on the circumstances, either three or six months (see s. 9(6)).

136. No s. 8(4) warrant may be renewed unless the Secretary of State believes that

the warrant continues to be necessary on grounds falling within s. 5(3) of RIPA: s. 9(2).

137. Further, by s. 9(3), the Secretary of State must cancel a s. 8(4) warrant if he is satisfied that the warrant is no longer necessary on grounds falling within s. 5(3).

138. Detailed provision is made for the modification of warrants and certificates by s. 10 of RIPA.

139. §5.17 of the Code requires records to be kept of copies of all renewals and modifications of s. 8(4) warrants / certificates, and the dates on which interception is started and stopped.

The handling and use of intercepted material and related communications data

140. Section 15(1)(a) of RIPA imposes a duty on the Secretary of State to ensure, in relation to s. 8(4) warrants (and s. 8(1) warrants), that such arrangements are in force as he considers necessary for securing that the requirements of ss. 15(2) and 15(3) are satisfied in relation to the intercepted material and any related communications data.[41] As regards material intercepted under the s. 8(4) regime, the requirements in ss. 15(2) and 15(3) apply both to intercepted material that may be read, looked at or listened to pursuant to s. 16 and the certificate in question and to material that may <u>not</u> be so examined.

141. In relation to intercepted material and any related communications data, the requirements of s. 15(2) are that:

> "*(a) the number of persons to whom any of the material or data is disclosed or otherwise made available,*
> *(b) the extent to which any of the material or data is disclosed or otherwise made available,*
> *(c) the extent to which any of the material or data is copied, and*
> *(d) the number of copies that are made,*
> *is limited to the minimum that is necessary for the authorised purposes.*"

142. The authorised purposes include those set out in s. 5(3), facilitating the carrying out of the functions of the Commissioner or the Tribunal and ensuring that a person conducting a criminal prosecution has the information he needs to determine what is required of him by his duty to secure the fairness of the prosecution: see s. 15(4).

143. As regards the uses to which (consistently with s. 15(2)) the Intelligence Services may put intercepted material and any related communications data, see s. 19(2) of the CTA (§47 above).

144. As regards s. 15(2)(b), the disclosure powers of each of the Intelligence Services are limited by the SSA, the ISA and the HRA (see §§38-50 above).

---

[41] This duty is subject to s. 15(6) (see §§156-157 below).

145. By s. 15(5) of RIPA, the s. 15(2) arrangements must include such arrangements as the Secretary of State considers necessary for securing that every copy of the material / data is stored, for so long as it is retained, in a secure manner.[42]

146. In relation to intercepted material and any related communications data, the requirements of s. 15(3) are that:

> *"…each copy of the material or data (if not destroyed earlier) is destroyed as soon as there are no longer any grounds for retaining it as necessary for any of the authorised purposes."*[43]

147. The term "copy" is defined widely for the purposes of s. 15. In particular, s. 15(8) provides:

> "*In this section 'copy', in relation to intercepted material or related communications data, means any of the following (whether or not in documentary form)-*
> *(a) any copy, extract or summary of the material or data which identifies itself as the product of an interception, and*
> *(b) any record referring to an interception which is a record of the identities of the persons to or by whom the intercepted material was sent, or to whom the communications data relates,*
> *and 'copied' shall be construed accordingly.*"

148. Chapter 6 of the Code expands on the nature of these safeguards. It begins by emphasising at §6.1 that all material intercepted under a s. 8(4) warrant (including related communications data) must be handled in accordance with the safeguards that the Secretary of State has approved under section 15.

149. The Code then provides further information about the s. 15 safeguards. As regards the dissemination of intercepted material and any related communications data, §6.4-6.5 provide:

> "*6.4 The number of persons to whom any of the material*[44] *is disclosed, and the extent of disclosure, must be limited to the minimum that is necessary for the authorised purposes set out in section 15(4) of [RIPA]. This obligation applies equally to disclosure to additional persons within an agency, and to disclosure outside the agency.*[45] *It is enforced by prohibiting disclosure to persons who do not hold the required security clearance, and also by the need-to-know principle: intercepted material must not be disclosed to any person unless that person's duties, which must relate to one of the authorised purposes, are such that he needs to know*

---

[42] The seventh data protection principle imposes a similar obligation, insofar as the intercepted material amounts to personal data.

[43] Insofar as intercepted material amounts to personal data, the same obligation is in substance also imposed by virtue of the fifth data protection principle.

[44] It is apparent from the drafting of §6.1 of the Code that references in Chapter 6 to "the material" and "the intercepted material" are to the material intercepted under an interception warrant, including any related communications data, and that therefore those terms do not bear the technical meaning given to them in s. 20 of RIPA.

[45] This aspect of the Code makes clear that intercepted material may be disclosed to other public authorities.

about the material to carry out those duties.[46] *In the same way only so much of the material may be disclosed as the recipient needs; for example if a summary of the material will suffice, no more than that should be disclosed.*

6.5 The obligations apply not just to the original interceptor, but also to anyone to whom the material is subsequently disclosed. In some cases this will be achieved by requiring the latter to obtain the originator's permission before disclosing the material further. In others, explicit safeguards are applied to secondary recipients."

150. Further, as §6.9 of the Code makes clear, arrangements regarding personnel security impose strict limits on who may gain access to intercepted material and any related communications data:

"*Each intercepting agency maintains a distribution list of persons who may have access to intercepted material or need to see any reporting in relation to it. All such persons must be appropriately vetted. Any person no longer needing access to perform his duties should be removed from any such list. Where it is necessary for an officer of one agency to disclose material to another, it is the former's responsibility to ensure that the recipient has the necessary clearance.*"

151. The Government's policy on security vetting was announced to Parliament by the then Prime Minister in 1994. The policy was most recently set out in a Cabinet Office booklet dated July 2010, "*HMG Personnel Security Controls*". In practice, the policy ensures that those who may have access to intercepted material and any related communications data have been rigorously vetted.

152. §6.6 of the Code explains the restrictions and safeguards that apply to copying:

"*Intercepted material may only be copied to the extent necessary for the authorised purposes set out in section 15(4) of [RIPA]. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of interception, and any record referring to an interception which is a record of the identities of the persons to or by whom the intercepted material was sent. The restrictions are implemented by requiring special treatment of such copies, extracts and summaries that are made by recording their making, distribution and destruction.*"

153. The safeguards in relation to storage and destruction are addressed in §§6.7 and 6.8 respectively:

"*6.7 Intercepted material, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of security clearance. This requirement to store intercept product securely applies to all those who are responsible for the handling of this material, including communications service providers ....*

[46] Thus, for instance, if GCHQ intercepted the communication of a terrorist suspect of interest to an intelligence officer that revealed that the terrorist suspect was planning to travel to London but also that the suspect's cousin was shortly to become a father, then only the former part of the communication would be disclosed to the intelligence officer.

6.8 Intercepted material, and all copies, extracts and summaries which can be identified as the product of an interception, must be securely destroyed as soon as it is no longer needed for any of the authorised purposes. If such material is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid under section 15(3) of [RIPA]."

154. Although the full details of the s. 15 safeguards cannot be made public, they are made available to the Commissioner (§6.1 of the Code) who is required to keep them under review (see s. 57(2)(d)(i)). Further, to facilitate oversight by the Commissioner, each intercepting agency is required to keep a record of the arrangements for meeting the requirements of sections 15(2) and (3) (see §5.17 of the Code). Any breach of the arrangements must be reported to the Commissioner (§6.1 of the Code), and if the Commissioner considers that the arrangements have proved inadequate in any relevant respect he must report this to the Prime Minister (see s. 58(3)).

155. The Commissioner's advice and approval was sought and given in respect of the documents constituting the s. 15 arrangements either before or shortly after 2 October 2000 (when RIPA came into force): §15 of the Commissioner's Annual Report for 2000. In practice, the advice of the Commissioner is sought when any substantive change is proposed to the s. 15 arrangements that apply under the s. 8(4) regime.

156. Finally, as regards s. 15, it is to be noted that s. 15(6) expressly recognises the possibility that intercepted material and related communications data may be shared with foreign States. By s. 15(6):

"*Arrangements in relation to interception warrants which are made for the purposes of subsection (1) –*

(a) shall not be required to secure that the requirements of subsections (2) and (3) are satisfied in so far as they relate to any of the intercepted material or related communications data, or any copy of any such material or data, possession of which has been surrendered to any authorities of a country or territory outside the United Kingdom; ..."

157. Instead, the s. 15(1) arrangements must secure that possession of the intercepted material and data (or copies thereof) is only surrendered to authorities of a country or territory outside the United Kingdom if it appears to the Secretary of State that requirements corresponding to those in ss. 15(2)-(3) will apply, to such extent (if any) as the Secretary of State thinks fit and that, in effect, appropriate restrictions are in place as regards the potential use of any of the intercepted material in proceedings outside the United Kingdom. See s. 15(6)(b) and s. 15(7).

158. The criminal law also protects the confidentiality of information obtained pursuant to an interception warrant:

158.1 Where an interception warrant has been issued or renewed, s. 19(1) of RIPA imposes a duty on, among others, every person holding office under the Crown to keep secret "everything" in the intercepted

material, together with any related communications data. Subject to certain limited defences (including the defence under s. 19(9)(b), that the disclosure was confined to a disclosure authorised by the warrant or the person to whom the warrant is or was addressed), it is an offence for a person to make a disclosure to another of anything that he is required to keep secret under s. 19. Any disclosure of intercepted material or related communications data in breach of the s. 15 arrangements would constitute a criminal offence under s. 19 (unless, exceptionally, one of the defences in s. 19 applied). The maximum penalty for this offence is a fine and five years imprisonment. See s. 19(4) of RIPA.

158.2 Under s. 4(1) of the OSA, it is a criminal offence for a person who is or has been a Crown servant or government contractor to disclose, without lawful authority, any information, document or other article to which s. 4 of the OSA applies and which is or has been in his possession by virtue of his position as such. By virtue of s. 4(3)(a) of the OSA, s. 4 of the OSA applies to any information obtained under the authority of an interception warrant. A conviction under s. 4 of the OSA can lead to a fine or a term of imprisonment for up to two years: s. 10(1) of the OSA.

158.3 By s. 8 of the OSA, it is also an offence for members of the Intelligence Services to fail to take reasonable care to prevent unauthorised disclosure of *e.g.* documents that contain intercepted material (or related communications data). See §56 above.

159. Finally, as regards handling and use, the practical effect of s. 17 of RIPA is that neither intercepted material nor any related communications data can ever be admitted in evidence in criminal trials. (The equivalent prohibition in s. 17 for civil proceedings is subject to the closed material procedure in Part 2 of the JSA.)

Oversight mechanisms in the s. 8(4) regime

160. There are three principal oversight mechanisms in the s. 8(4) regime:

160.1 the Commissioner (see §§161-174 below);

160.2 the ISC (see §§61-68 above); and

160.3 the Tribunal (see §§69-76 above, and §§175-178 below).

The Commissioner

161. The Commissioner provides an important means by which the exercise by the Intelligence Services of their interception powers under RIPA may be subject to effective oversight whilst maintaining appropriate levels of confidentiality regarding those activities.

162. The Prime Minister is under a duty to appoint a Commissioner (see s. 57(1) of

RIPA). By s. 57(5), the person so appointed must hold or have held high judicial office, so as to ensure that he is appropriately independent from the Government. The Commissioner was Sir Paul Kennedy until 31 December 2012, when Sir Anthony May was appointed.

163. Under s. 57(7), the Commissioner must be provided with such technical facilities and staff as are sufficient to ensure that he can properly carry out his functions. Those functions include those set out in s. 57(2), which provides in relevant part:

> "*…the [Commissioner] shall keep under review-*
> *(a) the exercise and performance by the Secretary of State of the powers and duties conferred or imposed on him by or under sections 1 to 11;*
> *…*
> *(d) the adequacy of the arrangements by virtue of which-*
> *(i) the duty which is imposed on the Secretary of State…by section 15*[47]*…*
> *[is] sought to be discharged*."

164. 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: s. 58(1).

165. In practice, the Commissioner visits each agency that is empowered to conduct interception twice a year. Before each such visit he obtains a full list of extant warrants and warrants that have been modified or cancelled since his last visit. He then randomly selects warrants from the list and, during the visit, examines the warrants and the supporting paperwork. He discusses the rationale for the warrant (and its benefits) with agency staff. He is also able to view the product of any interception. (See §6.2 of the Commissioner's 2012 Annual Report, which is the most recent report that is available.) The Commissioner has reviewed s. 8(4) warrants in this manner in the past.

166. The Commissioner also meets with the relevant Secretaries of State (see §6.6 of the Commissioner's 2012 Annual Report).

167. Important reporting duties are imposed on the Commissioner by s. 58. It is an indication of the importance attached to this aspect of the Commissioner's functions that reports are made to the Prime Minister.

168. The Commissioner is by s. 58(4) under a duty to make an annual report to the Prime Minister regarding the carrying out of his functions. Pursuant to s. 58(6), a copy of each annual report (redacted, where necessary, under s. 58(7)) must be laid before each House of Parliament. In this way, the Commissioner oversight functions helps to facilitate Parliamentary oversight of the activities of the Intelligence Services (including by the ISC). The Commissioner's practice is to make annual reports in open form, with a closed confidential annex for the benefit of the Prime Minister going into detail on any matters

[47] This is a reference to both the s. 15 and the s. 16 arrangements, as the latter are required by s. 15(1)(b).

which cannot be discussed openly.

169. Further, s. 58 provides:

> *"(2) If it at any time appears to the [Commissioner]-*
> *(a) that there has been a contravention of the provisions of this Act in relation to any matter with which the Commissioner is concerned, and*
> *(b) that the contravention has not been the subject of a report made to the Prime Minister by the Tribunal,*
> *he shall make a report to the Prime Minister with respect to that contravention.*
> *(3) If it at any time appears to the [Commissioner] that any arrangements by reference to which the duties imposed by [section 15]…have sought to be discharged have proved inadequate in relation to any matter with which the Commissioner is concerned, he shall make a report to the Prime Minister with respect to those arrangements*."

S. 58(5) grants the Commissioner power to make, at any time, any such other report to the Prime Minister on any other matter relating to the carrying out of his functions as he thinks fit.

170. In §6.5.1 his latest Annual Report (the 2012 Annual Report) the Commissioner stated that "GCHQ staff conduct themselves with the highest levels of integrity and legal compliance". In §6.5.2 of that report, he observed that "officers working for SIS conduct themselves in accordance with the highest levels of ethical and legal compliance". As regards the Security Service, §6.5.4 of the 2012 Annual Report records:

> "*I was again impressed by the attitude and expertise of the staff I met who are involved in the interception of communications and I am satisfied that they act with the highest levels of integrity*."

171. In addition, the Commissioner is required by s. 57(3) to give the Tribunal:

> "*…such assistance (including his opinion as to any issue falling to be determined by the Tribunal) as the Tribunal may require-*
> *(a) in connection with the investigation of any matter by the Tribunal; or*
> *(b) otherwise for the purposes of the Tribunal's consideration or determination of any matter*."

172. The Tribunal is also under a duty to ensure that the Commissioner is apprised of any relevant claims / complaints that come before it: s. 68(3).

173. The Commissioner's oversight functions are supported by the record keeping obligations that are imposed as part of the s. 8(4) regime. See §§116, 124, 133, 139 and 154 above; and §5.17 of the Code. His oversight functions are further supported by the obligation to report any breaches of the ss. 15 and 16 arrangements pursuant to §6.1 of the Code (see §§133 and 154 above).

174. In practice, all the agencies that are empowered to conduct interception have arrangements in place with the Commissioner to report errors that arise in their interception operations. The Commissioner addresses such errors in his

annual reports (see *e.g.* §6.4 of his 2012 Annual Report).

The Tribunal and interception under s. 8(4) warrants

175. As regards the s. 8(4) regime, the following specific aspects of the Tribunal's jurisdiction are of particular relevance (in addition to the broader jurisdictional heads set out in §70 above):

175.1 The Tribunal has exclusive jurisdiction to consider claims under s. 7(1)(a) of the HRA that relate to conduct for or in connection with the interception of communications in the course of their transmission by means of a telecommunication system:

(a) which has taken place with the authority, or purported authority of an interception warrant (ss. 65(2)(b), 65(3)(d), 65(5)(b), 65(7)(a) and 65(8)(a) of RIPA); or
(b) which has taken place in circumstances where it would not have been appropriate for the conduct to take place without an interception warrant or without proper consideration having been given to whether such authority should be sought (ss. 65(2)(a), 65(3)(d), 65(5)(b), 65(7)(b) and 65(8)(a) of RIPA).

175.2 The Tribunal may consider and determine any complaints by a person who is aggrieved by any conduct for or in connection with the interception of communications in the course of their transmission by a telecommunication system which he believes to have taken place in relation to him, to any of his property, to any communications sent by or to him, or intended for him, or to his use of any telecommunications service or system and to have taken place:

(a) with the authority, or purported authority of an interception warrant (ss. 65(2)(b), 65(4), 65(5)(b), 65(7)(a) and 65(8)(a) of RIPA); or
(b) in circumstances where it would not have been appropriate for the conduct to take place without an interception warrant or without proper consideration having been given to whether such authority should be sought: ss. 65(2)(b), 65(4), 65(5)(b), 65(7)(b) and 65(8)(a) of RIPA).

176. The Tribunal may thus entertain any ECHR claim or public law complaint about the operation or alleged operation of the s. 8(4) regime. This may include investigating whether the Intelligence Services have complied with the ss. 15 and 16 safeguards in any particular case.

177. Under s. 67(7) of RIPA, the Tribunal may (in addition to awarding compensation or making any other order that it thinks fit) make an order quashing or cancelling any warrant and an order requiring the destruction of any records of information which has been obtained in exercise of any power conferred by a warrant.

178. Further, where a claimant / complainant succeeds before the Tribunal and

the Tribunal's determination relates to any act or omission by or on behalf of the Secretary of State, or to conduct for which any warrant was issued by the Secretary of State, the Tribunal is by s. 68(5) of RIPA required to make a report of their findings to the Prime Minister.

The issues of pure law suitable for determination at a Legal Issues Hearing

179. It is submitted that the following issues of pure law can be identified from the Grounds advanced by Privacy International and Liberty:

Issue (iii)

Is the s. 8(4) regime sufficiently "foreseeable" for the purposes of the "in accordance with the law" requirement in Art. 8(2), including as regards the conditions on which and the circumstances in which persons in the United Kingdom are liable to have their communications intercepted and as regards conditions on which and the circumstances in which intercepted material and related communications data may be disclosed to a foreign intelligence agency?

Issue (iv)

Does the possibility that intercepted material and related communications data derived from interception under a s. 8(4) warrant may be supplied to the US Government give rise to a breach of the "necessity" requirement in Art. 8(2)?

Issue (v)

Does the fact that s. 8(4) warrants are neither issued by judges nor require the prior approval of judges give rise to a breach of the "necessity" requirement in Art. 8(2)?[48]

Issue (vi)

Does the absence of a requirement that s. 8(4) warrants target specific individuals or premises give rise to a breach of the "necessity" requirement in Art. 8(2)?

Issue (vii)

Is the "necessity" requirement in Art. 8(2) breached because interception under the s. 8(4) regime may in principle involve (i) the interception (and subsequent recording) of communications and related communications data without there being any reason to suspect that the communications of the individuals in question are relevant to national security, serious crime and/or the economic well-being of the United Kingdom, and (ii) the intercepted material so obtained being processed to determine whether (pursuant to s. 16 and the certificate in question) it may be read, looked at or listened to by one or more persons?

[48] The issue is phrased in this way as the Respondents anticipate that this is the thrust of Privacy International's complaint. As explained below, the Tribunal ensures that there is "judicial control" over the issuing of warrants.

Issue (viii)

Does the s. 8(4) regime unlawfully discriminate against EU citizens who are not UK nationals (for the purposes of Art. 18(1) TFEU) and/or unlawfully discriminate against non-UK nationals (for the purposes of Art. 14 as read with Art. 8)?

180. The remaining grounds of claim do not give rise to pure issues of law which are suitable for determination at a Legal Issues Hearing. Rather, these grounds of claim turn on factual assertions that are neither confirmed nor denied, and which are relevant to the determination of the "necessity" issues raised.[49] It follows that they must - as necessary - be investigated and considered by the Tribunal in closed session in the light of such relevant closed evidence, if any, as is filed by the Respondents.[50] The Respondents invite the Tribunal to investigate these grounds of claim in closed session after holding an Legal Issues Hearing. Nevertheless, in the interests of transparency, the Respondents have set out in §§160-178 above what can openly be said regarding the oversight mechanisms upon which they would as necessary[51] propose to rely for the purpose of establishing, as regards the s. 8(4) regime, that there exists (in all the circumstances) "*adequate and effective guarantees against abuse*" for the purposes of the "necessity" requirement (*Weber* at §106). They have also set out in §§12-14 above an open statement of the value of interception operations.

181. In addition, the Tribunal can in principle also investigate in closed session:

181.1 if any communications were intercepted, whether in fact any related communications data were disclosed or used in any other way;

181.2 if any communications were intercepted, whether in fact any of those communications were "read, looked at or listened to" by any person or persons;

181.3 if they were "read, looked at or listened to", whether they were retained, disclosed or used in any other way; and

181.4 in the light of all the relevant facts and circumstances, and irrespective of whether the overall s. 8(4) regime is proportionate for the purposes of Art. 8(2), whether any interception, examination, retention, disclosure or other use that in fact took place was a proportionate interference with the Claimants' Art. 8 rights.

182. It appears that the Claimants do not specifically invite the Tribunal to

[49] For the fact-specific nature of the "necessity" requirement, see §106 of *Weber*: the assessment whether there are adequate and effective guarantees against abuse "depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures...".

[50] The Respondent note, however, as regards Ground PI2.3(h), that the mere fact that an interception warrant can in principle be renewed indefinitely does not in itself give rise to Art. 8 incompatibility. See §161 of *Liberty*.

[51] *i.e.* assuming that some relevant s. 8(4) warrant or warrants are being used to conduct some relevant form of interception, which is neither confirmed nor denied.

investigate these matters, and correspondence from them dated 1 November 2013 suggests that they may in the event specifically request the Tribunal not to do so. Subject to an unequivocal request of this type, the Respondents would invite the Tribunal to investigate the matters set out in §181 above, as part of its investigative functions, and insofar as it is possible to do so given the limited information provided by the Claimants as to the "factors" which could be used in any searches by the Intelligence Services.

Issue (iii): Is the s. 8(4) regime sufficiently "foreseeable" for the purposes of the "in accordance with the law" requirement in Art. 8(2), including as regards the conditions on which and the circumstances in which persons in the United Kingdom are liable to have their communications intercepted and as regards conditions on which and the circumstances in which intercepted material and related communications data may be disclosed to a foreign intelligence agency?

183. The Claimants do not appear to dispute that the interference in question has a basis in domestic law, namely the s. 8(4) regime as summarised above. Similarly, the "accessibility" requirement is satisfied in that RIPA is primary legislation,[52] and the Code and the s. 8(4) Ruling are public documents. Again, the Claimants do not appear to dispute this.

184. As regards the foreseeability requirement, account must be taken of the special context of secret surveillance. In particular, as has consistently been recognised by the ECtHR, the requirement of foreseeability:

> "*...cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly*." (*Weber*, at §93. See also *e.g.* §67 of *Malone*)

185. This fundamental principle applies both to the interception of communications (so as to obtain intercepted material, *i.e.* the content of communications) and to the obtaining of related communications data (*i.e.* data that does not include the content of any communications). However, in other respects, the precise requirements of foreseeability differ for the interception of communications, on the one hand, and the obtaining of related communications data, on the other. Each is addressed in turn below.

Foreseeability of the interception of communications under the s. 8(4) regime

186. Subject to the principle set out in §184 above, there needs to be clear, detailed rules on the interception of communications to guard against the risk that such secret powers might be exercised arbitrarily (*Weber*, at §§93-94). As has already been noted, the ECtHR has developed the following set of six "minimum safeguards" that need to be set out in the domestic legal framework that governs the interception of communications, in order to ensure that the "foreseeability" requirement is met in this specific context:

> "*[1] the nature of the offences which may give rise to an interception order; [2] a*

[52] Similarly, the legislative provisions that make up the Intelligence Sharing regime are also contained in primary legislation.

definition of the categories of people liable to have their telephones tapped; [3] a limit on the duration of telephone tapping; [4] the procedure to be followed for examining, using and storing the data obtained; [5] the precautions to be taken when communicating the data to other parties; and [6] the circumstances in which recordings may or must be erased or the tapes destroyed ..." (*Weber*, at §95).

187. The *Liberty* case makes clear that it is not necessary that every provision be set out in primary legislation: the test is whether there is a sufficient indication of the safeguards "*in a form accessible to the public*" (see *Liberty*, at §§67-69, see also §157 of *Kennedy*).

188. §95 of *Weber* applies insofar as the s. 8(4) regime authorises the interception of communications. First, *Weber* concerned the German equivalent of the s. 8(4) regime. Secondly, §95 of *Weber* was applied in *Liberty*, which concerned the statutory predecessor to the s. 8(4) regime (namely, the regime for warrants under s. 3(2) of the Interception of Communications Act 1985).

189. As the ECtHR recognised in §95 of *Weber*, the reason why such safeguards need to be in a form accessible to the public is in order to avoid "abuses of power". This requirement is thus a facet of the more general principle that there must be adequate and effective guarantees against abuse. Accordingly, in determining whether the domestic safeguards meet the minimum standards set out in §95 of *Weber*, account should be taken of all the relevant circumstances, including:

> "*the authorities competent to ... supervise [the measures in question], and the kind of remedy provided by the national law ...*" (*Association for European Integration and Human Rights v. Bulgaria*, Appl. no. 62540/00, judgment of 28 June 2007, at §77.)

The Respondents rely in this regard on the oversight mechanisms set out in §§160-178 above.

190. The statutory predecessor of the s. 8(4) regime (in the Interception of Communications Act 1985) was found not to be "in accordance with the law" in *Liberty*. However, the reason for this conclusion was that, at the relevant time, the UK Government had not published further details of the interception regime in the form of a Code of Practice (see §§68-69 of *Liberty*). The s. 8(4) regime does not, of course, suffer from this flaw: the particular Code to which the ECtHR made reference in §68 of *Liberty* has been in force since 2002.

191. In the light of the above, the various safeguards listed in §95 of *Weber* are addressed in turn below.

(1) The "offences" which may give rise to an interception order

192. This requirement is satisfied by the RIPA regime (as set out in §§112-115 above). See *Kennedy* at §159. The Claimants do not appear to suggest otherwise.

(2) The categories of people liable to have their telephones tapped

193. As is clear from §97 of *Weber*, this second requirement in §95 of *Weber* applies both to the interception stage (which merely results in the obtaining / recording of communications) and to the subsequent selection stage (which results in a smaller volume of intercepted material being read, looked at or listened to by one or more persons).

194. As regards the interception stage:

194.1 As appears from s. 8(4)(a) and s. 8(5), a s. 8(4) warrant is directed primarily at the interception of external communications.

194.2 The term "communication" is sufficiently defined in s. 81. The term "external communication" is sufficiently defined in s. 20 and §5.1 of the Code. The s. 8(4) regime does not impose any limit on the types of "external communications" at issue, with the result that the broad definition of "communication" in s. 81 applies in full and, in principle, anything that falls within that definition may fall within s.8(5)(a) insofar as it is "external".

194.3 Further, as noted above, the s. 8(4) regime does not impose any express limit on number of external communications which may fall within "*the description of communications to which the warrant relates*" in s. 8(4)(a). §9 of the s. 8(4) Ruling makes clear, in this regard, that a s. 8(4) warrant may in principle result in "*the interception of all communications between the United Kingdom and an identified city or country*."

194.4 In addition, a s. 8(4) warrant may in principle authorise the interception of communications which are not "external" communications insofar as that is necessary in order to intercept the external communications to which the s. 8(4) warrant relates (see s. 5(6), and §121 above).

194.5 In the circumstances, and given that an individual should not be enabled "*to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly*" (see §184 above) and in the light of the available oversight mechanisms (see §189 above), the s. 8(4) regime sufficiently identifies the categories of people who are liable to have their communications intercepted.

195. As regards the selection stage:

195.1 No intercepted material will be read, looked at or listened to by any person unless it falls within the terms of the Secretary of State's certificate, and unless it is proportionate to do so in the particular circumstances of the case.

195.2 As regards the former, material will only fall within the terms of the certificate insofar as the examination of it is necessary on the grounds

in s. 5(3)(a)-(c). Those grounds are themselves sufficiently defined for the purposes of the foreseeability requirement (see §159 of *Kennedy*, and see also *mutatis mutandis* §160 of *Kennedy*: "*there is an overlap between the condition that the categories of person be set out and the condition that the nature of the offences be clearly defined*").

195.3 Further, s. 16(2), as read with the exceptions in s. 16(3)-(5A), place sufficiently precise limits on the extent to which intercepted material can be selected to be read, looked at or listened to according to a factor which is referable 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. Thus, by way of example, intercepted material could not in general be selected to be listened to by reference to a UK telephone number.

195.4 In the light of the above and, having regard - again - to the principle that an individual should not be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly and to the available oversight mechanisms (see §189 above), the s. 8(4) regime sufficiently identifies the categories of people who are liable to have their communications read, looked at or listened to by one or more persons. The Tribunal was, with respect, right to reach in substance this conclusion in the s. 8(4) Ruling.

(3) Limits on the duration of telephone tapping

196. The s. 8(4) regime makes sufficient provision for the duration of any section 8(1) warrant, and for the circumstances in which such a warrant may be renewed (see §§135-139 above, and §161 of *Kennedy*).

(4)-(5) The procedure to be followed for examining, using and storing the data obtained; and the precautions to be taken when communicating the data to other parties

197. Given §106 above, it is clear that the s. 8(4) regime may in principle involve the recording of intercepted material.

198. Insofar as the intercepted material cannot thereafter be read, looked at or listened to by a person pursuant to s. 16 (and the certificate in question), it is clear that it cannot be used at all. Prior to its destruction, it must of course be securely stored (§6.7 of the Code).

199. As regards the intercepted material that can be read, looked at or listened to pursuant to s. 16 (and the certificate in question), the applicable regime (see §140-159 above) is equally sufficient to satisfy the fourth and fifth foreseeability requirement in §95 of *Weber*. See §163 of *Kennedy*.

200. As regards the possible disclosure of intercepted material to foreign intelligence agencies in particular: the s. 8(4) regime expressly recognises the

possibility that such material / data may be disclosed to the authorities of foreign States, and makes specific provision for such disclosure (see §§156-157 above).

(6) The circumstances in which recordings may or must be erased or the tapes destroyed

201. S. 15(3) of RIPA and §6.8 of the Code make sufficient provision for this purpose: *Kennedy* at §§164-165.

Conclusion as regards the interception of communications

202. It follows that the s. 8(4) regime provides a sufficient public indication of the safeguards set out in §95 of *Weber*. As this is all that "foreseeability" requires in the present context (see §§95-102 of *Weber*), it follows that the s. 8(4) regime is sufficiently "foreseeable" for the purposes of the "in accordance with the law" requirement in Art. 8(2).

Foreseeability of the acquisition of related communications data under the s. 8(4) regime

203. *Weber* concerned the interception of the content of communications as opposed to the acquisition of communications data as part of an interception operation (see §93 of *Weber*). So far as the Respondents are aware, the list of safeguards in §95 of *Weber* (or similar lists in the other recent Strasbourg interception cases) has never been applied to powers to acquire communications data.

204. This is not surprising. As has already been noted, the covert acquisition of communications data is considered by the ECtHR to be less intrusive in Art. 8 terms than the covert acquisition of the content of communications. See *Malone* at §84. Thus, at a matter of principle, it is to be expected that the foreseeability requirement will be somewhat less onerous for covert powers to obtain communications data than for covert powers to intercept the content of communications (see the cases cited at §88 above).

205. Instead of the list of specific safeguards in *e.g.* §95 of *Weber*, the test is the general one whether the law indicates the scope of any discretion and the manner of its exercise with sufficient clarity "*to give the individual adequate protection against arbitrary interference*" (*Malone* at §68; *Bykov v. Russia* at §78). The same points as are made above, concerning the correct approach in a context in which there is no clear and constant jurisprudence of the ECtHR (*R (Ullah)* and other cases), apply here and are not repeated.

206. The s. 8(4) regime satisfies this test as regards the obtaining of related communications data:

206.1 The regime is sufficiently clear as regards the circumstances in which each of the Intelligence Services can obtain information related communications data. See, *mutatis mutandis*, §§192-194 and 196 above.

206.2 The regime equally contains sufficient clear provision regarding the subsequent handling, use and possible onward disclosure of information so obtained. See, *mutatis mutandis*, §§199-201 above.

207. In the alternative, if the list of safeguards in §95 of *Weber* applies to the obtaining of related communications data, then the s. 8(4) regime meets the requirements so imposed.

Issue (iv): Does the possibility that intercepted material and related communications data derived from interception under a s. 8(4) warrant may be supplied to the US Government give rise to a breach of the "necessity" requirement in Art. 8(2)?

208. As a matter of principle, a power to share intelligence with a foreign intelligence agency must plainly be capable of being "necessary" for the purposes of Art. 8(2). Privacy International cite no authority to suggest the contrary. Further, any disclosure must comply with s. 6(1) of the HRA, which itself requires that any interference that arises pursuant to the disclosure be proportionate.

209. It follows that the possibility of disclosure to a US agency does not give rise to a breach the Art. 8(2) requirement of necessity.

Issue (v): Does the fact that warrants under the s. 8(4) regime are neither issued by judges nor require the prior approval of judges give rise to a breach of the "necessity" requirement in Art. 8(2)?

210. S. 8(4) warrants are subject to judicial control insofar as the lawfulness of such warrants falls within the Tribunal's jurisdiction, and the Tribunal has power to quash such warrants (s. 67(7)(a)) and to order the destruction of records obtained under them (s. 67(b)(i)). (In addition, oversight is also provided by the Commissioner, who must hold or have held high judicial office.)

211. It is clear from §§167 and 169 of *Kennedy* that the Art. 8(2) "necessity" requirement does not require there to be prior judicial approval of interception warrants. Again, Privacy International cites no authority to the contrary.

Issue (vi): Does the absence of a requirement that s. 8(4) warrants target specific individuals or premises give rise to a breach of the "necessity" requirement in Art. 8(2)?

212. *Weber* concerned the German equivalent of the s. 8(4) regime, known as "strategic monitoring". Like the s. 8(4) regime, strategic monitoring does not involve interception that must be targeted at a specific individual or premises (see §4 of *Weber*, where strategic monitoring is distinguished from "individual monitoring"; and see the reference to 10% of all telecommunications being potentially subject to strategic monitoring in §110). Nevertheless, the applicants' challenge to the "necessity" of strategic monitoring was found by the ECtHR in *Weber* to be manifestly ill-founded

(§§137-138) and thus inadmissible.

213. It follows that the absence of a requirement that s. 8(4) warrants target specific individuals or premises equally does not give rise to a breach of the "necessity" requirement in Art. 8(2).

Issue (vii): Is the "necessity" requirement in Art. 8(2) breached because interception under the s. 8(4) regime may in principle involve (i) the interception (and subsequent recording) of communications and related communications data without there being any reason to suspect that the communications of the individuals in question are relevant to national security, serious crime and/or the economic well-being of the United Kingdom, and (ii) the intercepted material so obtained being processed to determine whether (pursuant to s. 16 and the certificate in question) it may be read, looked at or listened to by one or more persons?

214. *Weber* is also a complete answer to Issue (vii) insofar as it concerns the interception of communications.

Like the s. 8(4) regime, the strategic monitoring regime at issue in *Weber* involved two stages. In the case of strategic monitoring, the first stage was the interception of wireless communications (§26 of *Weber*) in manner that was not targeted at specific individuals (§4) and that might potentially extend to 10% of all communications (§110); and the second stage involved the use of "catchwords" (§32).

Against this background, the applicants complained, as part of their challenge to the "necessity" of strategic monitoring, that the intercepting agency in question was "entitled to monitor all telecommunications within its reach without any reason or previous suspicion" (§111).

However, and as already noted, the applicant's "necessity" challenge was not merely dismissed: it was found to be manifestly ill-founded.

215. It follows that the s. 8(4) regime similarly does not breach the Art. 8(2) necessity requirement by virtue of the fact that it may in principle involve the interception (and subsequent recording and processing) of communications without there being any reason to suspect that the communications of the individuals in question are relevant to national security, serious crime and/or the economic well-being of the United Kingdom.

216. Nor is there any principle to the effect that the "necessity" requirement is necessarily breached in the event that the State obtains the communications data of individuals who are not suspected of posing any threat to national security, etc., not least given the less private nature of communications data (*Malone* at §84). In any event, the requirements that are imposed on related communications data pursuant to s. 15 of RIPA are sufficient to ensure that such obtaining of communications data does not in itself give rise to a breach of the "necessity" requirement.

Issue (viii): Does the s. 8(4) regime unlawfully discriminate against EU citizens who are not UK nationals (for the purposes of Art. 18(1) TFEU) and/or unlawfully discriminate against non-UK nationals (for the purposes of Art. 14 as read with Art. 8)?

217. The discrimination complaint is based on a comparison between interception under s. 8(1) warrants and interception under s. 8(4) warrants.

218. In the s. 8(4) Ruling the Tribunal stated at §20.1:

> "*The basis for the two warrants is obviously different. This is because it is the more necessary for additional care to be taken with regard to interference with privacy by a Government in relation to domestic telecommunications, with regard to which it has substantial potential control; but also because its knowledge of, and certainly its control over, external communications is likely to be dramatically less. As a result the domestic regime, so far as permitted interception is concerned, is considerably tighter.*"

219. With respect, the Tribunal was right:

219.1 There are important practical differences between gathering intelligence on individual and organisations within the British Island and gathering intelligence on individuals and organisations that operate outside that jurisdiction. Within the British Islands, the Government has extensive powers and considerable resources available to investigate individuals and organisations that may *e.g.* threaten the interests of national security or commit serious crimes. It is therefore feasible for an interception regime to be adopted that requires individual addresses to be identified before interception can take place. Outside the British Islands, however, the ability of the Government to discover the identity and location of individuals and organisations which may represent a threat to national security, etc. is of, course, drastically reduced. In the light of this practical difficulty, it would not be possible to obtain adequate levels of intelligence about individuals and organisations operating outside the British Islands if interception could only be carried out in relation to communications going to or from specific addresses.[53]

219.2 As has already been noted, at the time of *Weber* German law had both

[53] Liberty attempts to distinguish the Tribunal's finding in §20(1) of the s. 8(4) Ruling by arguing, in effect, 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 s. 8(4) regime (§84 of Liberty's Grounds of Claim). The Respondents neither confirm nor deny the factual bases of this argument. But they note that, although a s. 8(4) warrant may authorise the interception of communications that are not external communications (on the basis that such interception is "necessary" under s. 5(6)(a)), s. 16 of RIPA places strict limits on the extent to which intercepted material (including material deriving from such communications) can be selected to be read, looked at or listened according to a factor which is referable to an individual who is known to be for the time being in the British Islands and which has at its purpose, or one of its purposes, the identification of material contained in communications sent by him, or intended for him.

a "strategic monitoring" regime and an "individual monitoring" regime. The former concerned only international telephone conversations via satellite connections or radio relay links (§97 of *Weber*). As such, it was in effect directed at the German equivalent of "external communications" as defined in RIPA. In other words, the German law at issue drew in substance the same distinction as is drawn in RIPA between the regime governing s. 8(1) warrants ("the s. 8(1) regime") and the s. 8(4) regime, yet it was found to be ECHR-compatible by the ECtHR.

220. It follows that there is justification for any disparate impact of the s. 8(4) regime in relation to EU Citizens (or non-UK nationals generally), as compared with UK nationals.

221. In any event, the EU discrimination claim cannot succeed because the s. 8(4) regime is outside the scope of application of the treaties.[54]

V. SUGGESTED DIRECTIONS

222. The Respondents invite the Tribunal to make the following directions, prior to any directions hearing:

222.1 Within 21 days of service of this Response, the Claimants shall confirm in writing whether the Issues for the Legal Issues Hearing that are identified in this Response are agreed and, to the extent that they are not, shall set out the pure issues of law which they propose should be determined at that hearing. The Claimants to be at liberty to file Replies by the same date.

222.2 Within 14 days thereafter the parties to file and serve their suggested directions for the management of the Claims up to and including the Legal Issues Hearing.

223. For the avoidance of doubt, the Respondents submit that the Tribunal does not have power to appoint "an investigator" (as suggested in §2(d) of Privacy International's letter of 25 October 2013). However, the Respondents respectfully suggest that the Commissioner (*i.e.* the Interception of Communications Commissioner) and Intelligence Services Commissioner are likely to be able to assist the Tribunal in the investigation of these Claims. The Respondents propose that in due course the two Commissioners be directed to assist in the closed session investigation of the Claims that will take place

[54] Contrary to §57 of Privacy International's Statement of Grounds, *Huber v. Germany* C-524/06 [2008] ECR I-9705 at §§69-81 is not authority to the contrary. *Huber* concerned a German system for processing the personal data of EU citizens who were not nationals of Germany who were resident in Germany. The German system thus fell within Art. 12(1) EC (now Art. 18(1) TFEU) read in conjunction with Art. 18 EC (the right to move and reside in the EU, now Art. 21 TFEU). By contrast, the s. 8(4) regime does not treat differently EU citizens (or other non-UK nationals) who are within the British Islands as compared with UK nationals who are within the British Islands.

after the Tribunal has published its rulings on the pure issues of law considered at the Legal Issues Hearing.

224. Further, as regards the suggestion in (among other places) Privacy International's letter of 25 October 2013 that a special advocate be appointed: the Rules make no provision for this, and both the Procedural Ruling and *Kennedy* confirm that the appointment of a special advocate is not necessary in Tribunal proceedings. However, if appropriate, the Tribunal can appoint an Advocate to the Tribunal (as it has done in the past) in order to assist it in any closed investigation and/or closed hearing that it decides to hold.

225. The Respondents would be content for the Tribunal to hold a public *inter partes* directions hearing to determine the procedure to be adopted in the two Claims. They respectfully submit (in common with Privacy International) that any directions hearing be listed on a date when all counsel are able to attend, given the specialist nature of the proceedings. At any directions hearing, the Respondents will propose that the two Claims be formally joined.

JAMES EADIE QC
BEN HOOPER

15 November 2013

Appendix

The pure issues of law suitable for determination at a Legal Issues Hearing, and the Respondents' overall position on each them

Issue (i)

Does the Intelligence Sharing regime satisfy the requirement in Art. 8(2) that any interference be "in accordance with the law"?

Yes.

Issue (ii)

Does the Intelligence Sharing regime ensure that the obtaining, retention and disclosure of information by the Intelligence Services pursues one or more legitimate aims for the purposes of Art. 8(2)?

Yes.

Issue (iii)

Is the s. 8(4) regime sufficiently "foreseeable" for the purposes of the "in accordance with the law" requirement in Art. 8(2), including as regards the conditions on which and the circumstances in which persons in the United Kingdom are liable to have their communications intercepted and as regards conditions on which and the circumstances in which intercepted material and related communications data may be disclosed to a foreign intelligence agency?

Yes.

Issue (iv)

Does the possibility that intercepted material and related communications data derived from interception under a s. 8(4) warrant may be supplied to the US Government give rise to a breach of the "necessity" requirement in Art. 8(2)?

No.

Issue (v)

Does the fact that s. 8(4) warrants are neither issued by judges nor require the prior approval of judges give rise to a breach of the "necessity" requirement in Art. 8(2)?

No.

Issue (vi)

Does the absence of a requirement that s. 8(4) warrants target specific individuals or premises give rise to a breach of the "necessity" requirement in Art. 8(2)?

No.

Issue (vii)

Is the "necessity" requirement in Art. 8(2) breached because interception under the s. 8(4) regime may in principle involve (i) the interception (and subsequent recording) of communications and related communications data without there being any reason to suspect that the communications of the individuals in question are relevant to national security, serious crime and/or the economic well-being of the United Kingdom, and (ii) the intercepted material so obtained being processed to determine whether (pursuant to s. 16 and the certificate in question) it may be read, looked at or listened to by one or more persons?

No.

Issue (viii)

Does the s. 8(4) regime unlawfully discriminate against EU citizens who are not UK nationals (for the purposes of Art. 18(1) TFEU) and/or unlawfully discriminate against non-UK nationals (for the purposes of Art. 14 as read with Art. 8)?

No.