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

PRIVACY INTERNATIONAL

Claimant

and

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

Respondents

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

LIBERTY

Claimant

and

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

Respondents

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

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

Claimants

and

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

Respondents

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

AMNESTY INTERNATIONAL LIMITED

Claimant

and

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

Respondents

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

BYTES FOR ALL

Claimant

and

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

Respondents

THE RESPONDENTS' SKELETON ARGUMENT ON THE PRELIMINARY ISSUES OF LAW

Contents

Glossary

The British Islands	The UK, the Channel Islands and the Isle of Man (see s. 5 of and Sch. 1 to the Interpretation Act 1978)
The Claimants	All the Claimants in all five of the joined Claims
The Code	The current Interception of Communications Code of Practice, issued on 1 July 2002 under s. 71 of RIPA
The Commissioner	The Interception of Communications Commissioner, appointed under s. 57(1); currently Sir Anthony May
Communications data	Certain data, as per the definition in ss. 21(4), 21(6) and 21(7) of RIPA, that relates to a communication but does not include its contents
The CTA	The Counter-Terrorism Act 2008
The DPA	The Data Protection Act 1998
External communication	A communication "sent or received outside the British islands" (see s. 20 of RIPA, and §5.1 of the Code)
GCHQ	The Government Communications Headquarters
The HRA	The Human Rights Act 1998
The Intelligence Services	As *per* the definition in s. 81(1) of RIPA: the Security Service, SIS and GCHQ
The Intelligence Sharing and Handling Regime	The statutory regime (set out in the Appendix) that governs the sharing of intelligence between the Intelligence Services and foreign intelligence agencies, and the handling and use of intelligence obtained as a result
Intercepted material	In relation to an interception warrant, "the contents of any communications intercepted by an interception to which the warrant relates" (see s. 20 of RIPA)
An interception warrant	A warrant issued in accordance with s. 5 of RIPA
Internal communication	A communication that is not an external communication (the term is not defined in RIPA itself, but it is a convenient shorthand)
The ISA	The Intelligence Services Act 1994

The ISC	The Intelligence and Security Committee of Parliament
The JSA	The Justice and Security Act 2013
NCND	Neither confirm nor deny
The Original Open Response	The Respondents' Open Response dated 15 November 2013 to the Claims brought by Privacy International and Liberty
The OSA	The Official Secrets Act 1989
The Procedural Ruling	The Tribunal's procedural ruling of 22 January 2003 in IPT/01/62 and IPT/01/77
The Respondents	All the Respondents in all five of the joined Claims
RIPA	The Regulation of Investigatory Powers Act 2000
The Rules	The Investigatory Powers Tribunal Rules 2000, SI 2000/2665
A s. 8(1) warrant	An interception warrant that complies with s. 8(2)-(3) of RIPA
The S. 8(4) Regime	The statutory regime (set out in the Appendix) that governs the interception of external communications and the handling and use of the intercepted material and communications data obtained as a result
The S. 8(4) Ruling	The Tribunal's ruling of 9 December 2004 in IPT/01/77
A s. 8(4) warrant	An interception warrant issued under the S. 8(4) regime that complies with ss. 8(4)-(6) of RIPA
SIS	The Secret Intelligence Service
The SSA	The Security Service Act 1989

References in the form "[*B *number* / *tab* / *page**]" are to the two bundles containing the Exhibit to Charles Farr's witness statement, dated 16 May 2014, for the Respondents (Exhibit CF1)

References to that witness statement and to the witness statements of Cindy Cohn (dated 27 September 2013, served in the *Big Brother Watch* proceedings in Strasbourg), Eric King (dated 8 June 2014) and Ian Brown (dated 27 September 2013, served in *Big Brother Watch*) are given in the form [*Witness *paragraph(s)**]

I. INTRODUCTION

1. The first set of preliminary issues of law (Issues (i)-(iii)) concern the possibility that the Intelligence Services might in principle obtain communications and communications data from the UK Government's closest intelligence ally, namely the US, that the US has itself obtained under Prism and/or the upstream collection programme.

2. As the Commissioner noted in his 2013 Annual Report:

> *"...information lawfully obtained by interception abroad is not necessarily available by interception to an interception agency here. In many cases it will not be available."* [*B2/14/914*]

3. The Claimants do not suggest that the Intelligence Services should never seek to obtain communications and communications data from their US counterparts. Instead, at their most extreme, their allegations raise the spectre of the Intelligence Services using Prism and upstream collection to conduct "*bulk*" surveillance of the UK population. But Prism and upstream collection are targeted rather than "*bulk*" programmes. Further, the ISC has found that GCHQ did not circumvent or attempt to circumvent UK law in its access to Prism.

4. The true position is as follows. There is a clear need for the Intelligence Services to be able to share intelligence - on a proportionate basis - with foreign intelligence partners. The Intelligence Sharing and Handling Regime permits such sharing, and appropriately governs the handling and use of intelligence (including communications and communications data) so obtained. It is thus "*in accordance with the law*" for the purposes of Art. 8(2) of the ECHR.

5. The second set of preliminary issues of law (Issues (iv)-(xi)) relate to the UK's ability to obtain communications and communications data under the S. 8(4) Regime and the alleged "*Tempora*" programme, in relation to which the Claimants make a series of ECHR complaints.

6. Given *Weber and Saravia v. Germany* (2008) 46 EHRR SE5, it is clear that the ECtHR is not opposed in principle to a regime of this type. Further, as the Commissioner has acknowledged, and as Parliament was aware when it enacted RIPA, <u>some</u> form of S. 8(4) Regime is in fact a practical necessity as regards external communications. The S. 8(4) Regime reflects these practical constraints, whilst imposing appropriate safeguards and oversight mechanisms. Thus, like the Intelligence Sharing and Handling Regime, it is also "*in accordance with the law*" for Art. 8(2) purposes, and otherwise ECHR-compatible in the various respects relevant to the preliminary issues of law.

7. Finally, as regards procedure (Issues (xii)-(xiv)), the Respondents are not obliged to depart from the ordinary NCND stance in relation to the alleged "*Tempora*" programme, and the Tribunal does not have power to direct the Respondents to disclose further information or evidence in open, or to make open admissions, etc. This is not a surprising result given the highly sensitive

intelligence context. Nor is it an inconvenient one: the preliminary issues of law can be determined without the Respondents needing to depart from NCND or disclose further material in open.

II: THE CLAIMANTS' FACTUAL ALLEGATIONS

8. The agreed factual premises address the possibility that the Claimants' communications or communications data might in principle have been obtained by the Intelligence Services, either from the US Government, or as the result of interception under the S. 8(4) Regime. The factual premises do not address either the scope or scale of the alleged interception of communications by the US or UK; or the nature of any interception programmes (save at a very general level); or the scope or scale of intelligence sharing between the US and UK. The reason is obvious. Those matters are not and cannot in any sense be agreed.

9. Notwithstanding that, the Claimants' skeletons invite the Tribunal to rule on the legal issues on the basis of extreme, and at times outlandish, factual assertions about the scope, scale and nature of US and UK interception programmes and intelligence sharing. Thus, it is said for example that the Government can obtain "*virtually all communications of UK residents from the Intelligence Services of other states*"[1], that "*all or most internet and telephone communications…are now being collected, stored and analysed by the Security and Intelligence Services*"[2], that "*the NSA is able to access a large majority of the world's communications and communications data*"[3] and that the "*US engages in mass surveillance of UK citizens*"[4]. Such assertions are presented as matters of established fact, against which the legal issues fall to be determined. It is even said in the same breath both that (correctly) "*neither the precise detail of the US's UPSTREAM interception and PRISM programs, nor the manner in which its product is obtained by the UK, requires determination*"; but that also it can properly be "*assumed*" that as a result of Prism and upstream collection the "*NSA will be able to access the majority of web-searches, emails and other internet communications sent or undertaken in the UK*".[5]

10. It is not for the Tribunal to make rulings of fact on these matters. The Respondents do not invite it to do so, it does not need to do so and it should not do so. Nevertheless, it is important to recognise that the assertions presented by the Claimants as matters of established fact are flatly contradicted by publicly available material, including from the US Government. No assumption can or should be made as to the truth of any of the Claimants' broad assertions about the intelligence-gathering activities of, or intelligence sharing between, the US or UK Governments, save to the extent that they are publicly avowed by the Governments themselves.

11. By way of example only, the Claimants assert both in their witness statements and skeleton arguments that Prism and upstream collection involve the "*bulk*" interception of communications, including the internal communications of UK residents, with no legal protection for non-US persons (see *e.g.* Cohn §11), the entire contents of which are then made fully available

[1] Privacy International's skeleton argument, §2.
[2] Privacy International's skeleton argument, §3.
[3] Privacy International's skeleton argument, §48.
[4] Amnesty's skeleton argument, §15(g)(i).
[5] Privacy International's skeleton argument, §52.

to the UK Intelligence Agencies[6]. Those assertions, however, are wholly contrary to material from the US Government that is before the Tribunal. See in particular (i) a report of 18 April 2014 of the NSA Director of Civil Liberties and Privacy Office, "*NSA's Implementation of Foreign Intelligence Surveillance Act Section 702*" [*B1/11/247*]; (ii) a paper from the Director of National Intelligence of 8 June 2013, "*Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*" at [*Vol. D/37*]; and (iii) a paper of 9 August 2013 from the National Security Agency, "*The National Security Agency: Missions, Authorities, Oversight and Partnerships*" at [*Vol. D/131*]. The latter documents are within Ms Cohn's own exhibit; and nowhere in her witness statement does she assert that they are inaccurate; in fact, she relies on their contents[7]. On the basis of that material, the position is rather that:

11.1 The NSA's collection authorities stem from two key sources: Executive Order 12333 and FISA [*Vol. D/132*]. All collection under any authority must be undertaken for foreign intelligence and counterintelligence purposes [*Vol. D/132*].

11.2 Prism and upstream collection are undertaken under the authority of FISA [*B1/11/252-253*].

11.3 Both Prism and upstream collection require an NSA analyst to identify a specific non-US person located outside the US (*e.g.* a person belonging to a foreign terrorist organisation[8]) as a "target", and to obtain a unique identifier associated with that target, such as an email address, to be used as a tasked "*selector*" [*B1/11/251-253*].

11.4 The analyst must verify the connection between the target and the selector; and must document (a) the foreign intelligence information expected to be acquired; and (b) the information that would lead a reasonable person to conclude that the selector was associated with a non-US person outside the US. That documentation must be reviewed and approved or denied by two senior NSA analysts [*B1/11/251-252*].

11.5 Under Prism, service providers are compelled to provide the NSA with communications to or from such approved selectors. Under upstream collection, service providers are required to assist the NSA lawfully to intercept communications to, from, or about, approved selectors [*B1/11/252-253*].

11.6 Thus, neither Prism nor upstream collection entails bulk interception. Moreover, both programmes entail a detailed, recorded and audited process identifying particular selectors (such as phone numbers or email addresses) before interception can occur.

---

[6] See *e.g.* the many examples in Privacy International's skeleton argument at §72.

[7] See [*Cohn §§7 and 28*].

[8] It is necessary that the person in question be someone who has and/or is likely to communicate foreign intelligence information as designated in a certification [*B1/11/251*].

11.7 Both programmes are undertaken with knowledge of the service provider, and under procedures approved by the FISA Court. All information obtained is based upon a written directive from the Attorney General and the Director of National Intelligence, detailing the foreign intelligence categories within which access requests must fall. Any such written directive is reviewed annually by the FISA court [*Vol. D/37*] [*B1/11/249*].

11.8 The NSA has a compliance programme, designed to ensure that its activities are conducted in accordance with law and procedure; therefore, in the case of Prism and upstream collection, in accordance with section 702 FISA and associated requirements. Issues of non-compliance must be reported to the Office of the Director of National Intelligence and the Department of Justice for further reporting to the FISA Court and Congress, as required [*B1/11/256*].

12. Furthermore, the Claimants' assertion that the Intelligence Services effectively obtain wholesale bulk communications from the US about UK citizens, with no oversight, is not only contrary to the Commissioner's finding that the British Intelligence agencies do not receive intercept material about British citizens from the US, which could not lawfully be acquired by intercept in the UK [*B2/14/914 at §6.8.1*]; but is also contrary to the contents of the UKUSA Intelligence Agreement at [*B1/7/135*]. The agreement provides for the unrestricted sharing of "*foreign communications*". Privacy International asserts (skeleton argument, §50) that "*for material obtained by the US, communications relating to British residents will be 'foreign communications'*". That is wrong. On the face of the UKUSA agreement, "*foreign communications*" are defined so as to exclude communications of the UK (and the US): see [*B1/7/140 and 198-199*].

13. The above are examples only of issues on which the Claimants make bold factual assertions, which are not borne out by the evidence. As already noted, the Respondents do not ask the Tribunal to make any findings on these specific (and sensitive) factual issues. However, they illustrate the danger of assuming that the Claimants' factual analysis in this regard is accurate.

III. PRISM / UPSTREAM COLLECTION

Agreed factual premises:

"1. The US Government's "Prism" system collects foreign intelligence information from electronic communication service providers under US court supervision. The US Government's "upstream collection" programme obtains internet communications under US court supervision as they transit the internet.

2. The Claimants' communications and/or communications data (i) might in principle have been obtained by the US Government via Prism (and/or, on the Claimants' case, pursuant to the "upstream collection" programme) and (ii) might in principle have thereafter been obtained by the Intelligence Services from the US Government. Thereafter, the Claimants' communications and/or communications data might in principle have been retained, used or disclosed by the Intelligence Services (a) pursuant to a specific request from the intelligence services and/or (b) not pursuant to a specific request from the intelligence services."

Issue (i): "In light of factual premises (1) and (2) above, does the statutory regime as set out in paragraphs 36-76 of the [Original Open Response] satisfy the Art. 8(2) 'in accordance with the law' requirement?"

14. For the reasons that follow, the Respondents submit that the answer to Issue (i) is, **yes**.

15. The statutory regime set out in §§36-76 of the Original Open Response is for convenience referred to as "the Intelligence Sharing and Handling Regime". An updated version of those paragraphs is at §§1-46 of the Appendix.

16. Before considering whether the Art. 8 interferences are "*in accordance with the law*" for Art. 8(2) purposes, it is necessary to identify the interferences at issue.

Identifying the Art. 8 interferences at issue

17. The Respondents maintain the usual "neither confirm nor deny" position as regards (i) whether any of the Claimants' communications and/or communications data have in fact been obtained by the US Government via Prism or upstream collection, and, if any communications and/or communications data have in fact been so obtained, (ii) whether those communications / data have been disclosed by the US Government to the Intelligence Services.

18. It follows that the Art. 8 interferences that need to be considered are not those that will have arisen if any relevant steps have in fact been taken in relation to the Claimants. Contrast the reference in §19 of Liberty's skeleton argument to the Respondents' actions interfering with the Claimants' Art. 8 rights.

19. Rather, the interferences at issue are those that arise as a result of the mere

existence of the Intelligence Sharing and Handling Regime and the fact that that regime might in principle have been used in order to obtain and thereafter use the Claimants' communications and/or communications data (assuming they had been obtained by the US).

20. This is the well-established approach of the ECtHR in cases involving intelligence matters (see *e.g.* §78 of *Weber*). It underpins agreed factual premise (2), which merely recognises the "in principle" possibility of relevant steps being taken in relation to the Claimants, and it obviates the need for the Tribunal - at this stage in the proceedings - to determine the likelihood that any relevant steps may have in fact been taken. (Contrast §4(e) of Amnesty's skeleton argument, where it is said to be "highly likely" that Prism and Upstream have been used to intercept / obtain Amnesty's communications and communications data.)

The "in accordance with the law" requirement

21. 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.)

22. The interferences at issue plainly have "*some basis*" in domestic law, namely the statutory provisions in the Intelligence Sharing and Handling Regime which would in principle provide the domestic law *vires* for the obtaining and subsequent use of the communications and communications data in issue (assuming that this was "*necessary*" for one or more of the functions of the Intelligence Service in question, and proportionate for the purposes of s. 6(1) of the HRA).[9]

23. Further, those statutory provisions are plainly "*accessible*".

24. In relation to "*foreseeability*" in this context, the essential test, as recognised in §68 of *Malone v. UK* (1984) 7 EHRR 14, 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. Further, this essential test must always be read subject to the important and well-established principle that the foreseeability requirement cannot mean

[9] There is no Strasbourg authority for the proposition that the relevant statutory provisions must expressly refer to any particular type of intelligence, such as intercepted communications / communications data, in order for there to be a sufficient basis in domestic law for obtaining such intelligence from a foreign intelligence agency for Art. 8(2) purposes. (Compare §24 of Liberty's skeleton argument.)

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* at §67; *Leander v. Sweden* (1987) 9 EHRR 433, at §51; and *Weber*, at §93.

26. In addition to the overarching - and necessarily somewhat general[10] - statutory scheme, detailed internal arrangements[11], guidance and policies plainly assist in guarding against "*arbitrary interference*" for the purposes of the essential test in §24 above. Yet, given the principle in §25 above, Art. 8 plainly does not require all such internal arrangements, guidance and policies to be published (see also Farr §§55-61, and see §§41-42 below). It follows, first, that the Tribunal can and should have regard to the internal arrangements, guidance and policies of the Intelligence Services when determining compliance with the "*in accordance with the law*" requirement; and, secondly, that the Tribunal should do so in closed session.

27. Overall, the Intelligence Sharing and Handling Regime satisfies the essential test in §24 above.

28. Given ss. 1-2 of the SSA, ss. 1-2 and 3-4 of the ISA (§§3-11 of the Appendix) and s. 6(1) of the HRA, the regime is sufficiently clear as regards the circumstances in which each of the Intelligence Services can **obtain** information (including in the form of communications / communications data) from foreign intelligence agencies, whether pursuant to a request or otherwise. See *Esbester v. UK* (1994) 18 EHRR CD72, *Hewitt v. UK* (1992) 14 EHRR 657 and *Redgrave v. UK*, Appl. No. 20271/92, 1 September 1993.

29. Thus, it is clear that *e.g.* GCHQ may in principle - as part of its function (in s. 3(1)(a) of ISA) of obtaining information derived from communications systems[12] - obtain communications and communications data from a foreign intelligence agency if that is both "*in support of the prevention or detection of serious crime*" (s. 3(2)(c) of ISA) and proportionate for that purpose under s. 6(1) of the HRA. Similarly, SIS may in principle *e.g.* obtain information (including communications and communications data) from a foreign intelligence agency that relates to the actions of persons outside the British Islands (s. 1(1)(a) of ISA) insofar as that is "*in the interests of national security,*

foreseeability purposes in §159 of *Kennedy v. UK* (2011) 52 EHRR 4. Thus, even on the assumption that the more recent interception cases apply in the present context (for which, see §§35-45 below), it is clear that the provisions governing the obtaining of information are sufficiently foreseeable. Indeed, in certain respects, the functions of the Intelligence Services are more tightly defined (see *e.g.* s. 1(2) of the SSA, and 1(2)(a) and 3(2)(a) of the ISA, as compared with s. 5(3)(a) of RIPA[13]). Further, Liberty's argument that the term "national security" is a protean concept (skeleton argument, §31) does not advance its case. The same argument was rejected at §159 of *Kennedy* by the ECtHR, which noted that "*By the nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance*". Further, the necessarily somewhat general statutory provisions (*c.f. S and Marper v. UK* (2009) 48 EHRR 50, at §96) are in turn supplemented by more detailed internal arrangements, guidance and policies, the detail of which cannot be publicly revealed.

31. Liberty also complains that it is "*circular*" to rely on the HRA in this regard (skeleton argument, §34). It is not. The issue is whether the relevant domestic law indicates the scope of any discretion and the manner of its exercise with sufficient clarity. For this purpose, the Respondents are entitled to rely on the accessible statutory obligation imposed on the Intelligence Services by s. 6 of the HRA to act proportionately, having regard to the aim pursued, when undertaking an activity that interferences with Art. 8 of the ECHR (or, for that matter, Art. 10). This is a domestic law constraint on the exercise of the powers in question, and it must be counted along with the other domestic law constraints in the SSA and ISA.[14]

32. For its part, Privacy International focuses on the possibility that the Intelligence Services might obtain communications (and related communications data) passing between to two individuals, "A" and "B", who are both in London (skeleton argument, §§59-77). As to this:

    32.1 Privacy International's arguments do not suggest that the Intelligence Sharing and Handling Regime is inappropriate insofar as it in principle permits the Intelligence Services to obtain, from foreign intelligence agencies, communications of individuals located outside the British Islands. This is the more usual factual context.

    32.2 This implicit concession is rightly made. It is plainly permissible for the Intelligence Services to seek the assistance of a foreign intelligence agency to obtain the communications of individuals located outside

[13] By s. 1(2) of the SSA, one of the Security Service's functions is "*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*" (emphasis added). Similarly, the statutory definition of the national security functions of SIS and GCHQ refer to "*the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom*" (emphasis added). Compare s. 5(3)(a) of RIPA, which identifies "*the interests of national security*" as a ground for interception, without further elaboration.

[14] See also §§25-29 of *Attorney General's Reference (No. 69 of 2013)* [2014] HRLR 7.

the British Islands if *e.g.* it is not technically feasible for the Intelligence Services themselves to undertake the interception in question under RIPA. In this regard, §6.8.6 of the Commissioner's 2013 Annual Report is to be noted:

> *"...information lawfully obtained by interception abroad is not necessarily available by interception to an interception agency here. In many cases it will not be available."* [*B2/14/914*]

Such a use of the Intelligence Sharing and Handling Regime does not amount to a deliberate circumvention of the safeguards and oversight mechanisms that are imposed in relation to RIPA interception warrants, and thus does not offend the well-establish *Padfield* principle[15].

32.3 As regards internal communications, such as those between A and B, circumstances may arise in which the Intelligence Services are unable to obtain all the communications in question under a RIPA interception warrant (this is for technical reasons, which are sensitive). In such circumstances, the Intelligence Services would of course need to conduct interception under a RIPA interception warrant to obtain those of A and B's communications that can be obtained directly by this process. But the Intelligence Services would also plainly be entitled to seek the assistance of a foreign intelligence agency to obtain some (or all) of the remainder without thereby circumventing the RIPA regime in contravention of the *Padfield* principle. As noted above, the ISC has confirmed that GCHQ did not circumvent UK law when accessing communications obtained via Prism; and the ISC further confirmed that "*in each case where GCHQ sought information the US, a warrant for interception, signed by a Minister, was already in place, in accordance with the legal safeguards contained in [RIPA]"* [*B1/16/346*].

32.4 The same analysis applies to communications data (see §26 of the Appendix).

33. Further, the Intelligence Sharing and Handling Regime is similarly sufficiently clear as regards the subsequent **handling, use and possible onward disclosure** of information (including communications / communications data) obtained by the Intelligence Services from foreign intelligence agencies.

33.1 **Handling and use** is addressed by (i) s. 19(2) of the CTA, as read with the statutory definitions of the Intelligence Services' functions (in s. 1 of the SSA and ss. 1 and 3 of ISA); (ii) the general proportionality constraints imposed by s. 6 of the HRA and - as regards retention periods in particular - the fifth data protection principle; and (iii) the seventh data protection principle (as reinforced by the criminal offence in ss. 1(1) and 8(1) of the OSA) as regards security measures

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

whilst the information is being stored.[16]

33.2 Thus, for instance, it is clear that information (including communications / communications data) obtained by *e.g.* SIS from a foreign intelligence agency, for national security purposes (within the meaning of s. 1(2)(a) of ISA), relating to the actions of persons outside the British Islands (within the meaning of s. 1(1)(a) of ISA) may be used by SIS in support of the prevention of serious crime that may be committed by persons outside the British Islands (s. 19(2) of the CTA as read with s. 1(1)(a) and s. 1(2)(c) of ISA), insofar as such use would be proportionate under s. 6(1) of the HRA. Indeed, when analysed in this way, it is difficult to see what public interest would be served by <u>further</u> constraining the powers of the Intelligence Services to use information. In particular, to return to the example just provided, it is difficult to see why SIS should not in principle be permitted to use the information in question in all cases in which such use would be proportionate in order to support the prevention or detection of serious crime within the scope of SIS's functions (as set out in s. 1(1) of the ISA).

33.3 Similarly, it is clear that information that has been obtained by *e.g.* SIS from a foreign intelligence agency, and that is being retained by SIS for its functions (as defined in s. 1(1) of the ISA) insofar as they are exercised for the purpose of national security (within the meaning of s. 1(2)(a) of ISA), cannot be retained for longer than is necessary for that purpose, given the fifth data protection principle.

33.4 Further, ss. 1-2 of the SSA and ss. 1-2 and 3-4 of the ISA, as read with ss. 19(3)-(5) of the CTA and s. 6(1) of the HRA, sufficiently address the circumstances in which the Intelligence Services may **disclose** information obtained from a foreign intelligence agency to others (see *mutatis mutandis* §§28-31 above). In addition, disclosure that is *e.g.* deliberately in breach of the "*arrangements*" for which provision is made in s. 2(2)(a) of the SSA and ss. 2(2)(a) and 4(2)(a) of the ISA would be criminal under s. 1(1) of the OSA.

33.5 Thus, for instance, it is clear that information obtained by *e.g.* SIS from a foreign intelligence agency, for national security purposes (within the meaning of s. 1(2)(a) of ISA), relating to the actions of a person outside the British Islands (within the meaning of s. 1(1)(a) of ISA) may be disclosed by SIS to another body for the purpose of the prevention of serious crime (s. 2(2)(a)(iii) of ISA and s. 19(4)(c)), insofar as such disclosure would be proportionate under s. 6(1) of the

[16] As to the fifth and seventh data protection principles, it is no answer to point to the national security exemption "available under section 28(2) [of the DPA]" (Liberty's skeleton argument, §35). As explained in §19 of the Appendix, the relevant certificates (which are publicly available) do <u>not</u> exempt the Intelligence Services from compliance with the fifth and seventh data protection principles (and the exemption arises under s. 28(1) of the DPA in any event). Contrast §61of Privacy International's skeleton argument, which (rightly) appears to accept that at least the fifth data protection principle applies.

HRA.

34. In addition:

34.1 When considering whether the Intelligence Sharing and Handling Regime is "*in accordance with the law*" and, in particular, "*foreseeable*", regard may properly be had to the available oversight mechanisms, namely, the ISC and the Tribunal (§§29-46 of the Appendix), and to their ability - as necessary - to consider both the appropriateness of confidential "arrangements" and other internal policies / guidance, and their application in particular cases (see, as regards the Tribunal, §26 above). Compare the references, as part of the "*in accordance with the law*" analysis, to the relevant oversight mechanisms in *Esbester* and *Hewitt*. See also *Kennedy*: when considering the general ECHR-compatibility of the RIPA s. 8(1) regime, the ECtHR at §§155-170 of *Kennedy* "*jointly*" considered the "*in accordance with the law*" and "*necessity*" requirements, and in particular analysed the available oversight mechanisms (at §§165-168) in tandem with considering the foreseeability of various elements of the regime (§§156-164). The approach in these cases on this issue is sound as a matter of principle, not least given that the essential test, as set out in §68 of *Malone*, seeks to guard against arbitrary inference. Oversight mechanisms plainly assist in this regard, and as such cannot sensibly be excluded from consideration.

34.2 The Tribunal's role is of particular significance in this regard. It provides a means of bringing claims and complaints in this sensitive intelligence context before a fully independent judicial body that has been specifically designed for that purpose.

34.3 Liberty's criticisms of the ISC and the Tribunal as oversight mechanisms at §36 of its skeleton are misplaced. Both are able to investigate issues arising under the Intelligence Sharing and Handling Regime, as is made plain by the ISC's Statement of 17 July 2013 [*B1/16/345*] and the present proceedings. Nor does the (non-binding) European Parliament Resolution of 12 March 2014 affect the true analysis. Both the ISC and the Tribunal have broad powers to require the Intelligence Services to provide them with relevant information (see §§34 and 45 of the Appendix), and neither have (to date) complained of having been granted insufficient access to such information. Compare also §105.1 below as regards the Commissioner's understanding of his own position.[17]

34.4 Further, the Tribunal should take into account the fact that the ISC has found that GCHQ "*has not circumvented or attempted to circumvent UK Law*" [*B1/16/346*][18] and has not found any abuse by the Intelligence

[17] In addition, the UK - like a number of other Member States - did not engage with the inquiry that preceded the Resolution.

[18] The investigation that preceded the ISC's Statement was thorough. See §5 of the Statement [*B1/16/345*].

Services of their powers to obtain communications and communications data, and that in his 2013 Annual Report the Commissioner similarly rejected the allegation that the Intelligence Services "*receive from US agencies intercept material about British citizens which could not lawfully be acquired by intercept in the UK ... and thereby circumvent domestic oversight regimes*" [*B2/14/914 at §§6.8.1-6.8.6*]. (Compare §168 of *Kennedy*.)

The more recent Strasbourg cases on interception do not assist the Claimants

35. 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).

36. However, it is important to appreciate that cases such as *Weber* and *Liberty* concern interception **by the respondent State**. The Claimants do not cite <u>any</u> 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 application of Art. 8 to cases of this latter type has never been considered in Strasbourg or in the domestic courts.

37. 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.

38. **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.

39. **Secondly**, there is no good reason to single out communications / communications data from other types of information that might in principle be obtained from a foreign intelligence agency, such as intelligence from covert human intelligence sources (as they would be termed under RIPA) or covert audio / visual surveillance. As Mr Farr explains, neither the sensitivity of the information in question, nor the ability of a person to predict the

possibility of an investigative measure being directed against him, distinguish communications and communications data from these other types of intelligence [*Farr §§27-30*]. The Claimants are unable to dispute this:

39.1 Liberty has no answer to this point (*c.f.* §40 of its skeleton argument). Nor does Amnesty address it in its skeleton argument.

39.2 Privacy International attempts to contrast interception with obtaining GPS location data for a person's car (skeleton argument, §71)[19]. But the examples that Mr Farr gave were different: an eavesdropping device in the home of the target in question, or a covert human intelligence source who has a friendship (or more intimate relationship) with the target. Privacy offers no reason for supposing that the intelligence derived from these types of operations would in some general sense be less personal or private than intelligence derived from interception.[20]

40. As there is no good reason to single out communications / communications data, the Claimants' argument proves too much. In particular, 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 and Handling 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 about an individual that derived from covert human intelligence sources, covert audio / visual surveillance or covert property searches. 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 (see Farr §§15-26).

41. **Thirdly**, it would plainly not be feasible (or, from a national security perspective, safe) 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. See Farr §§56-61:

41.1 The specific details would reveal sensitive intelligence-gathering capabilities and relationships, and gaps / shortcomings in them [*Farr §56*], and compare §67 of *Malone* (the requirement of foreseeability "*cannot mean than an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his*

[19] In particular, *Uzun* was concerned with such GPS location data. See §§12-13 of the judgment.

[20] See also §69 of Privacy International's skeleton, which is directed to comparing interception in the UK with surveillance or the use of covert human intelligence sources in the US; <u>not</u> with comparing interception in the US with surveillance or the use of covert human intelligence sources in the US.

conduct accordingly").

41.2 Further details may pose acute difficulties for liaison relationships with foreign intelligence agencies [*Farr §58*].

41.3 Operational flexibility would be limited by the inclusion of too much detail regarding intelligence sharing and handling arrangements [*Farr §59*].

41.4 Detailed provisions would quickly become outdated, and any amendments to ensure ongoing effectiveness would provide additional insights into the activities, methods and priorities of the Intelligence Services [*Farr §60*], contrary to §67 of *Malone*.

Further, the ECtHR has never suggested that this form of wide-ranging and detailed statutory scheme for intelligence sharing with foreign intelligence agencies is necessary (and see §96 of *S and Marper*).

42. As Mr Farr confirms at §61 of his statement, the difficulties summarised in §§41.1-41.4 above would equally arise even if the UK Government were somehow only required to publish more information about the obtaining of communications and communications data from foreign intelligence agencies, and their handling, use and possible onward disclosure.

43. 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, and there is no domestic right of appeal for either the Claimants or the Respondents. 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 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.

44. Thus, the test to be applied is whether the Intelligence Sharing and Handling 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). For the reasons given in §§28-33 above, that test is satisfied.

45. 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, having regard to §§39-42 above, the available oversight

mechanisms and the findings of the ISC and Commissioner (see §34 above).

Alleged positive obligations under Art. 8

46. Amnesty's skeleton argument at §§15-16 asserts that the Respondents have acted unlawfully in relation to Prism and the upstream collection programme, and contrary to various positive duties they are said to owe under Art. 8, because:

    46.1 They have failed to take positive action required to uphold the rights under Art. 8 of persons within the jurisdiction of the UK, by for example instituting some "*form of action to prevent the actions of US officials*", taking some "*sanction against US officials in respect of this mass surveillance of UK citizens*", or taking "*steps to award recompense for persons under the jurisdiction of the UK whose personal data has been obtained, stored and searched by US officials*" (§15).

    46.2 They have "*acquiesced or connived*" in acts of the United States which have violated the ECHR rights of individuals within the jurisdiction of the United Kingdom (§16).

47. There is a distinct air of unreality about these submissions. Amnesty does not (and cannot) explain how the UK could prevent the US from obtaining communications from US communications providers under s. 702 of FISA to protect the US's own national security. Nor does Amnesty explain on what basis the UK would be empowered to impose "*sanctions*" against the US; or why the UK should be expected to undermine the US's attempts to protect its own national security by informing subjects of US surveillance that their personal data had been obtained, stored or searched by US officials. The obvious likely effect of the sort of steps that Amnesty proposes would be an immediate end to any intelligence sharing relationship between the UK and US, as well as catastrophic damage to the relations between the US and the UK more generally.

48. In any event, Amnesty's arguments are hopeless as a matter of ECHR law.

49. US acts concerning Prism and upstream collection are acts carried out within the jurisdiction of the US (and under the supervision of the US courts), whether or not they involve interference with the electronic communications of persons who are located within the UK. They entail the imposition of legal duties upon service providers within the US, either to provide relevant electronic communications to the NSA, or to assist with their interception: see *e.g.* the Report of the NSA Director of Civil Liberties and Privacy Office concerning the implementation of s. 702 of FISA [*B1/11/252*].

50. The ECHR does not give rise to any obligation on the part of contracting states to secure that non-contracting states, acting within their own jurisdiction, respect the rights and freedoms guaranteed by the ECHR, even if the failure of such non-contracting states to do so may have adverse effects on persons within the jurisdiction of contracting states. See *Bertrand Russell Peace Foundation Ltd v. UK* (1978) 14 DR 117 at §124 and *R (Al Rawi) v. Secretary of*

State for Foreign and Commonwealth Affairs [2008] QB 289 at §§96-99 *per* Laws LJ giving the judgment of the Court of Appeal.

51. The *Bertrand Russell* case, which has never been doubted and which has been cited in many subsequent Strasbourg decisions, is particularly pertinent in this context. It concerned a complaint by the applicant peace foundation of breaches of Arts. 8 and 10 on the basis that the UK had refused to intervene or to pay compensation when the Soviet authorities had intercepted and interfered with the applicant's mail. The ECommHR dismissed the applicant's complaint as "*manifestly ill-founded*". The Commission stated that Art. 1 of the ECHR[21] had to be viewed against the general principle in Art. 34 of the Vienna Convention on the Law of Treaties that a treaty does not create either obligations or rights for a third party state without its consent; and that being so, the act or omission complained of (and not simply the victim of that act) must be within the jurisdiction of the contracting state.[22] So the UK was neither obliged to intervene with the Soviet authorities; nor to take steps to recompense the applicant as the victim of the Soviet authorities' acts (*Bertrand Russell* at p. 124).

52. Indeed, the *Bertrand Russell* case is also authority for a wider proposition, reflected in many subsequent Strasbourg decisions, and equally applicable here, that the ECHR imposes no positive obligation upon contracting states to espouse an applicant's complaints under international law, or otherwise intervene with the authorities of another state on his or her behalf: see e.g. *Kapas v. UK* , Appl. No. 12822/87, 9 December 1987, at §2, *Dobberstein v. Germany*, Appl. No. 25045/94, 12 April 1996, *M v. Italy* (2013) 57 EHRR 29 at §127 and *Al Rawi* at §96.

53. None of the cases cited in §15 of Amnesty's skeleton concerns the duties of a contracting state to prevent, or to compensate an applicant for, the acts of a third party state within its own jurisdiction; and none casts any doubt at all on the principles set out above.

54. Similarly, the authorities upon which Amnesty relies at §16 of its skeleton, concerning the acquiescence or connivance of the authorities of a contracting state in the unlawful acts of third parties, take its case no further. Those authorities deal with acts of third parties within the jurisdiction of the contracting state: see *e.g. El-Masri v. Macedonia* (2013) 57 EHRR 25 at §206. That is not this case.

55. Finally, Amnesty's submissions on alleged positive obligations at §§15-16 are based on a fundamentally misconceived approach to the issues that the Tribunal needs to determine. Amnesty's submissions at §§15-16 take as their

---

[21] Art. 1 of the ECHR provides:
"*The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention.*"

[22] The application of the Vienna Convention on the Law of Treaties to the ECHR is just one aspect of the more general proposition that the ECHR should so far as possible be interpreted in harmony with other rules of international law of which it forms part: see *e.g. Al-Adsani v. UK* (2002) 34 EHRR 11, at §55.

starting point the premise, which is neither before the Tribunal nor for the Tribunal to determine, that the US has acted unlawfully by obtaining the data of UK citizens (and in particular, has acted unlawfully according to principles of ECHR law, when the US is not a signatory to the ECHR). [23] The agreed issues on Prism and upstream collection require the Tribunal to consider the UK's Intelligence Sharing and Handling Regime. Those issues are not (nor could they be) based upon an assumption that the US has breached the rights of UK citizens by actions within its own jurisdiction, which is an issue for the US courts.

Issue (ii): "Given factual premise (2), does any obtaining, retention, use or disclosure of the Claimants' communications and communications data amount in itself to an interference with the Claimants' Art. 10 rights, if any?"

56. In principle, **Art. 10 inferences may arise on this basis**.

57. In particular, in the light of *Österreichische Vereinigung zur Erhaltung v. Austria*, Appl. No. 39534/07, 28 November 2013, the Respondents accept that, in the present context, non-governmental organisations engaged in the legitimate gathering of information of public interest in order to contribute to public debate may properly claim the same Art. 10 protections as the press.

58. In principle, therefore, the obtaining, retention, use or disclosure of the Claimants' communications and communications data may potentially amount to an interference with their Art. 10 rights, at least where the communications in question are quasi-journalistic ones, relating to their role as "social watchdogs".

59. Further, the Claimants may complain of an Art. 10 interference given the existence of the Intelligence Sharing and Handling regime, and the theoretical possibility that it may have been used in order to obtain and thereafter use the Claimants' communications and/or communications data (*c.f. Weber* at §§144-145).

Issue (iii) arises: "In light of factual premises (1) and (2) above, does the statutory regime as set out in paragraphs 36-76 of the Respondents' Open Response to the Claims brought by Liberty and Privacy International satisfy the Art. 10(2) 'prescribed by law' requirement?"

60. The need for the Art. 10 interferences to be "*prescribed by law*" for the purposes of Art. 10(2) adds nothing to the analysis of the "*in accordance with*

[23] Any such determination, quite apart from being contrary to the agreed factual premises, would also be contrary to the foreign Act of State doctrine, a long-standing principle of English public law. The classic statement of the principle is that of the US Supreme Court in *Underhill v. Hernandez* (1897) 168 US 250 at 252 (cited with approval in e.g. *R v. Jones (Margaret)* [2007] 1 AC 136, at §30 *per* Lord Bingham):

> *"Every sovereign State is bound to respect the independence of every other sovereign State, and the courts of one country will not sit in judgment on the acts of the government of another done within its own territory. Redress of grievances by reason of such acts must be obtained through the means open to be availed of by sovereign powers as between themselves."*

the law" requirement under Art. 8(2). See §147 of *Weber*.

61. Thus the answer to Issue (iii) is the same as the answer to Issue (i), namely, **yes**.

IV. THE ALLEGED "*TEMPORA*" INTERCEPTION OPERATION

Agreed Factual premises:

"3. The Claimants' communications might in principle have been intercepted in the United Kingdom under the s. 8(4) regime (as defined in the Original Open Response) and at least some of those intercepted communications might in principle have been 'read, looked at or listened to' by a person or persons under that regime.

4. The Claimants allege:

(a) the Intelligence Services operate a programme, described as Tempora, under which fibre optic cables are intercepted. This involves making available the contents of all the communications and communications data being transmitted through the fibre optic cables;

(b) the intercepted communications and communications data may be retained for an indefinite period and automatically searched through the use of a large number of search terms, including search terms supplied by the United States National Security Agency.

(c) The intercepted communications and communications data may then be further retained, analysed and shared with other public authorities."

Preliminary points

62. An updated version of the statutory regime set out in §§102-178 of the Original Open Response - *i.e.* the S. 8(4) Regime - is at §§47-122 of the Appendix.

63. For the reasons given in §§17-20 above, the Art. 8 interferences at issue are those that arise as a result of the mere existence of the S. 8(4) Regime and the fact that that regime might in principle have been used in order to obtain and thereafter use the Claimants' communications and/or communications data.

64. Five preliminary points should be noted at the outset:

64.1 some form of S. 8(4) Regime is a practical necessity;

64.2 the S. 8(4) Regime was designed on this basis, and with the internet in mind;

64.3 the existing Strasbourg interception case law - and in particular *Weber*, *Liberty* and *Kennedy* - supports the Respondents' position that the "*in accordance with the law*" requirement is satisfied;

64.4 by contrast, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and others C-293/12,* 8 April 2014, is not relevant to this issue; and

64.5 contrary to the Claimants' case, it remains the case that intercepting the communications (*i.e.* obtaining the content of communications) is

in general more intrusive - and is thus deserving of greater protection - than obtaining communications data.

65. Each is dealt with in greater detail below.

The practical necessity of some form of S. 8(4) Regime

66. The S. 8(4) Regime in principle permits a substantial volume of communications to be intercepted, and then requires the application of a selection process to identify a smaller volume of intercepted material that can actually be examined by persons, with a prohibition on the remainder being so examined (see §77 of the Appendix). To this extent, it differs from the regime that applies under s. 8(1) of RIPA, under which interception warrants target a specified person or single set of premises.

67. The crucial point is that this differences does not reflect some policy choice on the UK Government's part to undertake a programme of "*mass surveillance*" (*c.f.* §2 of Privacy International's skeleton argument) in circumstances where a s. 8(1) warrant would be perfectly well suited to acquiring the external communications that are needed for the purposes of national security, etc.

68. In truth, the UK Government has no choice in this regard. As the Commissioner has confirmed, following an "*in detail*" investigation of the relevant (and sensitive) technical background relating to the procedure under the S. 8(4) Regime:

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

Further, in the light of "*extensive practical and technical information provided*", the Commissioner has confirmed that:

> "*... it is not at the moment technically feasible to intercept external communications without a risk that some internal communications may also be initially intercepted.*" [*B2/14/906 at §6.5.52*]

69. As noted by the Commissioner, the technical details are sensitive. But this much can be said:

69.1 Interception occurs when the contents of a communication are "*made available*" to a person other than the sender or recipient (including by being obtained and recorded). (§50 of the Appendix.)

69.2 As Privacy International's witness Mr King explains, communications that are sent over the internet are broken down into small pieces, known as "*packets*", which are then "*transmitted separately, often through different routes, to the recipient, where the message is reassembled*" [*King §7*].

69.3 It follows that, in order to intercept a given communication that is travelling over the internet (say, an email), any intercepting agency will need to obtain all the packets associated with that communication, and reassemble them (as Mr King accepts at §48).

69.4 Further, the Claimants positively aver that discovering the ultimate recipient of an internet-based communication (such as an email) will require any intercepting agency "*to inspect the entirety of the packet, including the content of the communication*" [*King §47*] and will need to "*collect the entire sequence of packets and reconstruct them*" (emphasis added) [*King §48*]. In other words, the Claimants' case is that in order to discover the ultimate recipient of such a communication, any intercepting agency will have to intercept that communication (in terms of obtaining its content, if only for a short period).

69.5 Thus, on the Claimants' case, if an intercepting agency needs *e.g.* to obtain the external communications that are being sent to "C", an individual in Syria, whilst they were being transmitted over the internet, and the agency has access to a given communications "*link*" down which such communications might travel, the intercepting agency needs to intercept all communications that are being transmitted over that communications link - at least for a short time - in order to discover whether any are intended for C. Further, and again on the Claimants' case, as the packets associated with a given communication can taken different routes to reach their common destination, it may be necessary to intercept all communications over more than one communications link to maximise the chance of identifying and obtaining the external communications that are being sent to C in Syria.

69.6 The true position is somewhat more complicated (and the details are sensitive). But the Respondents can openly accept that the Claimants' account as referred to above applies to nearly all forms of internet-based communication.

70. Given §§69.5 and 69.6 above it is thus common ground that, at least for nearly all forms of internet-based communication, the only way to intercept those that are being sent to C is to intercept a substantially greater volume of communications (including, potentially, a volume of internal communications), and then apply a selection stage to identify the communications in question. In other words, it is common ground that the only practical way to find and reconstruct most external communication "needles" is to look through the communications "haystack".

71. This common ground has the following importance consequence: unless the Claimants' wish to submit that the Intelligence Services should not be able to obtain the external communications that are needed for the purposes of national security, etc., they must accept *some* form of interception regime that permits substantially more communications to be intercepted (including, potentially, internal communications) than are actually being sought. Or, to continue the analogy in §70 above, they must accept a regime that permits the

inspection of "haystacks".

72. In addition, as Mr Farr explains and as the Tribunal accepted in §20.1 of the S. 8(4) Ruling, there are important practical differences between the ability of the Intelligence Services to investigate individuals and organisations within the British Islands as compared with those abroad [*Farr §§142-147*]. The Claimants have no good answer to this simple and obvious point. (Privacy International's reference to the Parliament's stance in the 18th Century towards the then American colonies is plainly not to the point[24]; and see, further, §§160-161 below). These practical differences offer further justification for a regime of the form of the S. 8(4) Regime [*Farr §149*].

73. Finally, and *contra* Privacy International's arguments, the Respondents do not accept that a s. 8(4) warrant is properly analogous to a "*general warrant*". But, insofar as there are any superficial similarities, these are a necessary consequence of the practical points noted above.

The S. 8(4) Regime was designed with the internet in mind, and on the basis that some form of S. 8(4) Regime was required

74. The S. 8(4) regime was - to Parliament's knowledge - designed with the internet in mind, and Parliament was made aware of the issue noted in §§68-70 above. See Lord Bassam in Lords Committee (Hansard, 12 July 2000 at column 323):

> *"It is just not possible to ensure that only external communications are intercepted. That is because modern communications are often routed in ways that are not all intuitively obvious…. An internal communication--say, a message from London to Birmingham--may be handled on its journey by Internet service providers in, perhaps, two different countries outside the United Kingdom. We understand that. The communication might therefore be found on a link between those two foreign countries. Such a link should clearly be treated as external, yet it would contain at least this one internal communication. <u>There is no way of filtering that out without intercepting the whole link, including the internal communication.</u>*
>
> *Even after interception, it may not be practically possible to guarantee to filter out all internal messages. <u>Messages may well be split into separate parts which are sent by different routes. Only some of these will contain the originator and the intended final recipient</u>...."* [*B1/21/424*]

75. Unsurprisingly, given the above, the Commissioner concluded in his 2013 Annual Report that RIPA had not become "*unfit for purposes in the developing internet age*" [*B2/14/907 at §6.5.55*].

***Weber*, *Liberty* and *Kennedy* support the Respondents' position**

76. *Weber* concerned the German equivalent of the S. 8(4) Regime, known as "strategic monitoring". For present purposes three features of strategic monitoring are to be noted:

[24] See §21 of Privacy International's skeleton argument.

76.1 Like the S. 8(4) Regime, strategic monitoring did not involve interception that had to be targeted at a specific individual or premises (see §4 of *Weber*, where strategic monitoring was distinguished from "*individual monitoring*"; and see the reference to 10% of all telecommunications being potentially subject to strategic monitoring at §110).

76.2 Like the S. 8(4) Regime, strategic monitoring involved two stages. In the case of strategic monitoring, the first stage was the interception of wireless communications (§26 of *Weber*) in a manner that was not targeted at specific individuals and that might potentially extend to 10% of all communications; and the second stage involved the use of "*catchwords*" (§32). Against this background the applicants in *Weber* complained - as the Claimants do in these proceedings - that the intercepting agency in question was "*entitled to monitor all telecommunications within its reach without any reason or previous suspicion*" (§111).

77. Despite the above, the applicants' Art. 8 challenge in *Weber* to strategic monitoring was not merely rejected, it was found to be "*manifestly ill-founded*" (§§137-138) and thus inadmissible.

78. It follows that from the standpoint of the ECHR there is nothing in principle objectionable about:

78.1 an interception regime for external communications that is not targeted at specific individuals or premises; or

78.2 a two-stage interception regime for external communications that involves an initial interception stage which may in principle lead to a substantial volume of intercepted material being obtained, followed by a selection stage which serves to identify a subset of that material that can thereafter be examined.

79. This is unsurprising, not least given the first preliminary point addressed at §§66-72 above.

80. As to *Liberty*:

80.1 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*.

80.2 However, the reason for this conclusion was that, at the relevant time, the UK Government had not published any further details of the interception regime, in the form of a Code of Practice (see §69). In particular, the ECtHR noted in this regard that the Code under RIPA (that had been published by the time of the ECtHR's judgment) showed that "*it is possible for a State to make public certain details about the operation of a scheme of external surveillance without compromising*

national security." (§68, emphasis added.)

80.3 The s. 8(4) regime does not, of course, suffer from this flaw. The Code to which the ECtHR expressly made reference in §68 of *Liberty* remains in force.

80.4 Further, and significantly, the ECtHR did not conclude that Art. 8 required the UK Government to publish the Secretary of State's "*arrangements*" under s. 6 of the Interception of Communications Act 1985 (now ss. 15-16 of RIPA).

81. In *Kennedy* the ECtHR unanimously upheld the Art. 8-compatibility of the RIPA regime regarding s. 8(1) warrants. There are, of course, certain differences between that regime and the S. 8(4) Regime. However, there is also much that is similar, or identical, and thus *Kennedy* affords considerable assistance when considering the specific safeguards listed in §95 of *Weber*.

***Digital Rights Ireland* is irrelevant**

82. The Claimants rely upon the recent judgment of the CJEU in *Digital Rights Ireland*, to contend that a power permitting the mass interception of communications is not proportionate.[25]

83. *Digital Rights Ireland* concerned the lawfulness of Directive 2006/24/EC on Data Retention. Directive 2006/24/EC required communications service providers to retain all customer data for a period of not less than six months, and up to two years, so that it could be made available to law enforcement authorities. The CJEU held that the obligation to retain data in Arts. 3 and 6 of the Directive constituted an unjustified interference with the right to privacy in Art. 7 of the EU Charter of Fundamental Rights ("the Charter") and the right to protection of person data in Art. 8 of the Charter. The Claimants seek to apply those findings by analogy to the alleged "*Tempora*" programme.

84. The findings of the CJEU in *Digital Rights Ireland* cannot be read across to the present context, either as a matter of law or as a matter of fact. On a proper analysis, the judgment does not assist the Claimants' case in any way.

85. **First**, as a matter of law, the principles in *Digital Rights Ireland* cannot automatically be read across either to the interception of communications by State authorities, or to the use and disclosure of intercepted material / related communications data by State authorities, for the purposes of national security. Directive 2006/24/EC was an internal market meaasrt. eEC storccjjjvirtc,v()(ji tKm),5(

security (because data retention was for those purposes). In rejecting Ireland's arguments, the CJEU held, inter alia:

> *"81…the provisions of Directive 2006/24 are designed to harmonise national laws on the obligation to retain data (Article 3), the categories of data to be retained (Article 5), the periods of retention of data (Article 6), data protection and data security (Article 7) and the conditions for data storage (Article 8).*
> *82. By contrast, the measures provided for by Directive 2006/24 do not, in themselves, involve intervention by the police or law-enforcement authorities of the Member States. Thus, as is clear in particular from Article 3 of the directive, it is provided that service providers are to retain only data that are generated or processed in the course of the provision of the relevant communication services. Those data are solely those which are closely linked to the exercise of the commercial activity of the service providers.*
> *83. Directive 2006/24 thus regulates operations which are independent of the implementation of any police and judicial cooperation in criminal matters. It harmonises neither the issue of access to data by the competent national law-enforcement authorities nor that relating to the use and exchange of those data between those authorities. Those matters, which fall, in principle, within the area covered by Title VI of the EU Treaty, have been excluded from the provisions of that directive, as is stated, in particular, in recital 25 in the preamble to, and Article 4 of, Directive 2006/24.*[26]*"* (Emphasis added.)

87. **Secondly,** Directive 2006/24/EC required Member States to impose an unrestricted duty upon service providers to retain all data falling within Art. 5 of Directive 2006/24/EC for between six months and two years; yet contained no substantive or procedural conditions for the access to, and subsequent use of, that data. Indeed, that problem was at the heart of the CJEU's judgment in *Digital Rights Ireland*: see §61 of the judgment. No comparison can be drawn between that position, and the carefully crafted safeguards for the retention of intercepted material and related communications data in ss. 15 and 16 of RIPA, and the Code. Under those safeguards, for example: (i) any intercepted material and related communications data must be destroyed as soon as there are no longer grounds for retaining it for any "*authorised purpose*" pursuant to s. 15(3); (ii) the "*authorised purposes*" are tightly defined in s. 15(4); (iii) the number of persons to whom intercepted material or communications data is disclosed or made available, the extent to which it is disclosed or made available, the extent to which it is copied, and the number of copies that are made, are all limited to the minimum necessary for the "*authorised purposes*": s. 15(2) of RIPA; and (iv) s. 16 of RIPA imposes additional safeguards governing the access to material intercepted under a s. 8(4) warrant. (See, further, below).

---

[26] Recital 25 provides:

> *"This Directive is without prejudice to the power of Member States to adopt legislative measures concerning the right of access to, and use of, data by national authorities, as designated by them. Issues of access to data retained pursuant to this Directive by national authorities for such activities as are referred to in the first indent of Article 3(2) of Directive 95/46/EC fall outside the scope of Community law. However, they may be subject to national law or action pursuant to Title VI of the Treaty on European Union."* (Emphasis added.)

In line with Recital 25, Art. 4 of the Data Retention Directive leaves these matters to Member States.

88. Note also in this regard the Commissioner's findings in his 2013 Annual Report that "*none of the intercepting agencies retain or store for more than a short period the contents of intercepted communications which do not relate to a warranted target or which are of no legitimate interest*" and "*indiscriminate retention for long periods of unselected interception material (content) does not occur*" [*B2/14/866 at §3.53 and 867 at §3.55*].

Intercepting communications is in general more intrusive than obtaining communications data

89. The ECtHR recognised in §84 of *Malone* that it is less intrusive to obtain communications data than the contents of communications.

90. This remains the case even in relation to internet-based communications. For instance, obtaining the information contained in the "to" and "from" fields of an email (*i.e.* who the email is sent to, and who the email is sent by) will generally involve much less intrusion into the privacy rights of those communicating than obtaining the message content in the body of that email.

91. The Claimants seek to dispute this, in particular by reference to the possibility of aggregating communications data. (See *e.g.* §90(1) of Privacy International's skeleton argument, referring to King §§18-24; and Brown §§8-13).

92. It is by no means inevitable that aggregating communications data will yield information of any particular sensitivity. For instance, and to take a hypothetical example, the date, time and duration of telephone calls between an employee and his or her office are unlikely to reveal anything particularly private or sensitive, even if the aggregated communications data in question span many months, or even years.

93. Nevertheless, it is possible that aggregating communications data may in certain circumstances (and, potentially, with the addition of further information that is not communications data)[27] yield information that is more sensitive and private than the information contained in any given individual item of communications data. However, it is important to compare like with like. The issue is not whether *e.g.* 50 or 100 items of communications data relating to Syria-based C might - when aggregated - generate more privacy concerns that an intercepted communication sent or received by C. If aggregation is to be considered, then the comparison must be between 50 or 100 items of communications data relating to C and the content of 50 or 100 of C's communications. When the comparison is undertaken on a like-for-like basis, it is clear that §84 of *Malone* remains correct, even in an age of internet-

[27] See the example noted at Brown §10. The fact that a woman has called a particular telephone number, and that that telephone number belongs to someone with the title "*Dr*", are both forms of communications data (the latter being a form of subscriber information falling in principle within s. 21(4)(b)). But the fact the doctor in question is her gynaecologist cannot be derived from communications data (as opposed to the telephone call itself, or other information).

based communications. In particular, the content of communications continues to be generally more sensitive than the communications data that relates to those communications, and that is as true for aggregated sets of information as for individual items of information.

Issue (iv): "In light of the factual premises at paragraphs (3) and (4) above, does the statutory regime as set out in paragraphs 102-178 of the [Original Open Response] satisfy the Art. 8(2) 'in accordance with the law' requirement?"

94. The Respondents submit that the answer to Issue (iv) is, **yes**.

The "in accordance with the law" requirement

95. The Art. 8 interferences in question have a basis in domestic law, namely the S. 8(4) Regime.

96. Further, the "accessibility" requirement is satisfied in that RIPA is primary legislation[28] and the Code is a public document, and insofar as the S. 8(4)

"*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 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).

101. The *Liberty* case makes clear that it is not necessary that every provision / rule 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*).

102. §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 (see §76 above). Secondly, §95 of *Weber* was applied in *Liberty*, which concerned the statutory predecessor to the S. 8(4) Regime.

103. In the light of the above, the various safeguards listed in §95 of *Weber* are addressed - in turn - at §§106-116 below. Such a point-by-point analysis is a necessary part of determining compliance with the "*in accordance with the law*" requirement for interception. See *e.g.* the ECtHR's approach in §§159-164 of *Kennedy*, and *Weber* itself, at §§96-100. By contrast:

    103.1 The test is not whether, in one or more respects, the S. 8(4) Regime is somehow broader or less tightly defined then the German strategic monitoring regime at issue in *Weber* (not least because strategic monitoring satisfied the "*in accordance with the law*" requirement by some margin, in that the Art. 8 complaint in *Weber* was thrown out as "*manifestly ill-founded*": §138). Contrast §94 of Privacy International's skeleton argument.

    103.2 Nor is the test whether the UK Government might be able to publish at least <u>some</u> more details of the S. 8(4) Regime or impose at least <u>some</u> more constraints on the powers that are exercised under it (contrast the Claimants' arguments regarding the draft revised code of practice, at §§90-92 of Privacy International's skeleton argument and §67 of Liberty's skeleton argument).

104. 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 as necessary be taken of all the relevant circumstances, including any internal arrangements, guidance and policies that regulate or constrain the exercise of the powers in question (compare §26 above), and:

"*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, 28 June 2007, at §77.)

105. Thus, as in the case of the Intelligence Sharing and Handling Regime (see §34.1 above), the Respondents rely on the relevant oversight mechanisms, namely the Commissioner, the ISC and the Tribunal, and the relevant internal arrangements, guidance and policies of the Intelligence Services. The Respondents emphasise the following points:

105.1 The Commissioner (a former Lord Justice of Appeal) has himself stated that his investigations are "*thorough and penetrating*" and that he has "*no hesitation in challenging the public authorities wherever this has been necessary*" [*B2/14/896 at §6.3.3*]. As to his powers to compel disclosure / the provision of documents and information, the Commissioner has found "*that everyone does this without inhibition*" and that he is thus "*fully informed, or able to make [himself] fully informed about all interception ... activities ... however sensitive these may be*." [*B2/14/856 at §2.14*].[30]

105.2 The Commissioner regularly inspects the Intelligence Services and the work of senior officials and staff at the relevant Departments of State, and produces "*detailed*" written reports and recommendations [*Farr §§87-95*]. He also is empowered to investigate individual matters of concern, should he consider it appropriate to do so (see Sections 5-6 of the 2013 Annual Report [*B2/14/891*]).

105.3 Whilst the full details of the ss. 15 and 16 "*arrangements*" cannot safely be put into the public domain [*Farr §100*], (i) the Commissioner is required to keep them under review (s. 57(2)(d)(i) of RIPA), (ii) any breach of them must be reported to him (§6.1 of the Code) and (iii) in practice his advice is sought when any substantive change is proposed [*Farr §104*]. In addition, the Tribunal can and should consider them in closed session when determining ECHR-compliance.

105.4 The ISC is currently considering the adequacy of the "*current statutory framework governing access to private communications*" and the "*extent of the capabilities*" available to the Intelligence Services and their impact on people's privacy [*Farr §§74-76*].

105.5 As regards the Tribunal, a claimant does not need to be able to adduce cogent evidence that some steps have in fact been taken by the Intelligence Services in relation to him before his claim will be investigated.

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

106. This requirement is satisfied by s. 5 of RIPA, as read with the relevant

[30] See also §§6.1.1-6.1.2 of the Commissioner's 2013 Annual Report [*B2/14/893*].

definitions in s. 81 of RIPA and §5.4 of the Code (see §§55-58 in the Appendix). This follows, in particular, from a straightforward application of §159 of *Kennedy*.

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

107. 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).

108. As regards the interception stage:

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

108.2 The term "*communication*" is sufficiently defined in s. 81 of RIPA. The term "*external communication*" is sufficiently defined in s. 20 and §5.1 of the Code (see Issue (v) at §§123-136 below). 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*".

108.3 Further, 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) (see §67 of the Appendix). As §9 of the s. 8(4) Ruling makes clear, 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*." Similarly, during the Parliamentary debate on the Bill that was to become RIPA, Lord Bassam referred to intercepting the whole of a communications "*link*" (see §74 above, and contrast §79 of Liberty's skeleton argument).

108.4 In addition, a s. 8(4) warrant may in principle authorise the interception of internal 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) of RIPA, and the reference back to s. 5(6) in s. 8(5)(b) of RIPA (which latter provision needs to be read with s. 8(4)(a) of RIPA).[31] This point was also made clear to Parliament (see §74 above) and it has in any event been publicly confirmed by the Commissioner (see §68 above).

108.5 In the circumstances, and given that an individual should not be

[31] Liberty appears to have overlooked these provisions. See §86(4) of its skeleton argument: "*There is no indication on the face of the statute that the interception of communications 'not identified' by a section 8(4) RIPA warrant may nonetheless knowingly include internal communications*".

enabled "*to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly*" (see §97 above) and in the light of the available oversight mechanisms (see §104 above), the s. 8(4) regime sufficiently identifies the categories of people who are liable to have their communications intercepted.

109. As regards the selection stage:

109.1 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 (given s. 6(1) of the HRA) it is proportionate to do so in the particular circumstances of the case.

109.2 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) of RIPA. 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*").

109.3 Further, s. 16(2) of RIPA, 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 landline telephone number.[32]

109.4 As regards the Claimants' "*allegation*" in factual premise (4)(b) regarding NSA activity, any alleged access by the NSA at this stage (about which the Respondents adopt an NCND stance) would similarly be constrained in the same way by s. 16 of RIPA and, as it would amount to a disclosure by the Intelligence Service in question to another person, would similarly have to comply with s. 6(1) of the HRA and be subject to the constraints in ss. 1-2 of the SSA and ss. 1-2 and 3-4 of the ISA, as read with ss. 19(3)-(5) of the CTA.

109.5 The above provisions do not permit indiscriminate trawling, as the Commissioner has publicly confirmed [*B2/14/904 at §6.5.43*].

109.6 In the light of the above and, having regard - again - to the principle

[32] Liberty argues that s. 16(2) can be "*swept aside by the wide discretion given to the Secretary of State under section 16(3) RIPA*" (skeleton argument, §90(4)). In truth, the Secretary of State's power to modify a certificate under s. 16(3) so that intercepted material can be selected according to a factor that is referable to a particular identified individual is in substance as tightly constrained as his power to issue a s. 8(1) warrant, the ECHR-compatibility of which was confirmed by the ECtHR in *Kennedy*.

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 §104 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

110. 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 §§81-85 of the Appendix, and §161 of *Kennedy*).

111. The possibility that a s. 8(4) warrant might be repeatedly renewed does not alter the analysis (contrast §87(3) of Liberty's skeleton argument.) If, in all the circumstances, a s. 8(4) interception warrant continues to be necessary and proportionate under s. 5 of RIPA each time it comes up for renewal, then the Secretary of State may lawfully renew it. The Strasbourg test does not preclude this. Rather, the test is whether there are statutory limits on the operation of warrants, once issued. There are such limits here.

(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

112. Given §50 of the Appendix, it is clear that the s. 8(4) regime may in principle involve the recording of intercepted material.

113. Insofar as the intercepted material cannot 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). Further, and as has been publicly confirmed by the Commissioner, material that is "*filtered out*" at the selection stage is "*immediately discarded and ceases to be available*" [*B2/14/904 at §6.5.40*].

114. 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 is equally sufficient to satisfy the fourth and fifth foreseeability requirement in §95 of *Weber*. See §163 of *Kennedy*. In particular:

114.1 Such material can be used by the Intelligence Services only in accordance with s. 19(2) of the CTA, as read with the statutory definition of the Intelligence Services' functions (in s. 1 of the SSA and ss. 1 and 3 of the ISA) and only insofar as that is proportionate under s. 6(1) of the HRA. See also §6.6 of the Code as regards copying and §6.7 of the Code as regards storage (the latter being reinforced by the seventh data protection principle).

114.2 Further, s. 15(2) sets out the precautions to be taken when

communicating intercepted material that can be read, looked at or listened to pursuant to s. 16 to other persons (including foreign intelligence agencies: see §100 of the Appendix). These precautions serve to ensure *e.g.* that only so much of any intercepted material or related communications data as is "*necessary*" for the authorised purposes (as defined in s. 15(4)) is disclosed. The s. 15 safeguards are supplemented in this regard by §§6.4 and 6.5 of the Code (see §93 of the Appendix). In addition, any such disclosure must satisfy the constraints imposed by ss. 1-2 of the SSA and ss. 1-2 and 3-4 of the ISA, as read with ss. 19(3)-(5) of the CTA and s. 6(1) of the HRA. Further, and as in the case of the Intelligence Sharing and Handling Regime, a disclosure that is *e.g.* deliberately in breach of the "*arrangements*" for which provision is made in s. 2(2)(a) of the SSA and ss. 2(2)(a) and 4(2)(a) of the ISA would be criminal under s. 1(1) of the OSA.

114.3 As already noted, the detail of the s. 15 arrangements is kept under review by the Commissioner (see §105.3 above).

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

115. S. 15(3) of RIPA and §6.8 of the Code (including the obligation to review retention at appropriate intervals) make sufficient provision for this purpose: *Kennedy* at §§164-165. Both s. 15(3) and §6.8 are reinforced by the fifth data protection principle. See §18-21 of the Appendix.

116. Like the s. 15 arrangements, and as already noted, the detail of the s. 16 arrangements is kept under review by the Commissioner (see §105.3 above).

Conclusion as regards the interception of communications

117. 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

118. *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.

119. 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, and that

remains true in the internet age. 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 §38 above).

120. 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), subject always to the critical principle that the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to obtain, access and use his communications data so that he can adapt his conduct accordingly (*c.f.* §93 of *Weber*, and §67 of *Malone*). 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 (*Ullah* and other cases), apply here and are not repeated. §105 above is also repeated.

121. The S. 8(4) Regime satisfies this test as regards the obtaining of related communications data:

121.1 The S. 8(4) Regime is sufficiently clear as regards the circumstances in which the Intelligence Services can **obtain** information related communications data. See §§106-108 above, which applies equally here.

121.2 Once obtained, **access** to any related communications data is constrained by ss. 15(2)(a) and 15(2)(b) of RIPA (as read with s. 15(4)) and s. 6(1) of the HRA. As regards the Claimants' "*allegations*" in Factual Premise (4)(b), any access by the NSA at this stage (about which the Respondents adopt an NCND stance) would similarly be constrained in the same way by ss. 15(2)(a) and 15(2)(b) of RIPA (as read with s. 15(4)) (see §100 of the Appendix) and, as it would amount to a disclosure by the Intelligence Service in question to another person would similarly have to comply with s. 6(1) of the HRA and be subject to the constraints in ss. 1-2 of the SSA and ss. 1-2 and 3-4 of the ISA, as read with ss. 19(3)-(5) of the CTA.

121.3 Given the constraints in ss. 15 of RIPA and s. 6(1) of the HRA, communications data <u>cannot</u> be used (in combination with other information / intelligence) to discover *e.g.* that a woman of no intelligence interest may be planning an abortion (to use the example in Brown §10). This is for the simple reason that obtaining this information would very obviously serve none of the authorised purposes in s. 15(4). There is nothing unique about communications data (even when aggregated) here. Other RIPA powers, such as the powers to conduct covert surveillance and the use of covert human intelligence sources, might equally be said to be capable of enabling discovery of the fact that a woman of no intelligence interest may be planning an abortion (*e.g.* an eavesdropping device might be planted in her home, or a covert human intelligence source might be tasked to

befriend her). But it is equally clear that these powers could not in practice be used in this way, and for precisely the same reason: such activity would very obviously not be for the relevant statutory purposes (see ss. 28(3), 29(3) and 32(3) of RIPA).

121.4 This is also the answer to the speculative suggestion that there may be "*mass surveillance*" which is "*being used to develop much broader intelligence from the data of entire sections of populations*" (Liberty's skeleton argument, §7, fourth bullet point). It would be unlawful to use communications data to investigate a person of no intelligence interest. *A fortiori* it would be unlawful to use such data to investigate "*entire sections of populations*".

121.5 Further, there is good reason for s. 16 of RIPA covering access to intercepted material (*i.e.* the content of communications) and not covering access to communications data:

(a) In order for s. 16 to work as a safeguard in relation to individuals who are within the British Islands, but whose communications might be intercepted as part of the S. 8(4) Regime, the Intelligence Services need information to be able to assess whether any potential target is "*for the time being in the British Islands*" (for the purposes of s. 16(2)(a)). Communications data is a significant resource in this regard.

(b) In other words, an important reason why the Intelligence Services need access to related communications data under the S. 8(4) Regime is precisely so as to ensure that the s. 16 safeguard works properly and, insofar as possible, factors are not used at the selection that are - albeit not to the knowledge of the Intelligence Services - "*referable to an individual who is ... for the time being in the British Islands*".

121.6 The regime equally contains sufficient clear provision regarding the subsequent **handling, use and possible onward disclosure** by the Intelligence Services of related communications data. See, *mutatis mutandis*, §§114-116 above.

122. 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 given §121 above (and, as regards the limits on the duration of s. 8(4) warrants, §§110-111 above).

Issue (v): "Given the Claimants' allegations at factual premise (4), is the definition of 'external communications' within s.20 Regulation of Investigatory Powers Act 2000 sufficiently precise to be 'in accordance with the law' for the purposes of Art.8(2)?"

123. In the Respondents' submission, **yes**.

124. The meaning of an "*external communication*" for the purposes of Chapter I of

RIPA is stated in s. 20 of RIPA to be "*a communication sent or received outside the British Islands*". That definition is further clarified by §5.1 of the Code:

> "*External communications are defined by the Act to be those which are sent or received outside the British Islands. They include those 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*".

125. The Claimants complain that, in the context of modern electronic communications, the distinction between internal and external communications is insufficiently certain as to its scope and effect, and does not provide an effective safeguard against what is said to be a "general warrant". Thus, it is said, the distinction fails to meet the "*in accordance with the law*" requirement in Art. 8(2).

126. This complaint lacks merit:

126.1 First, the definition of an "*external communication*" is sufficiently clear in the circumstances.

126.2 Secondly, whilst in practice the analysis of whether an individual electronic communication is "internal" or "external" may be a difficult one (which can be conducted only with the benefit of hindsight), this has no bearing upon whether a specific communication is likely to be intercepted under the S. 8(4) Regime.

126.3 Thirdly, this issue similarly has no bearing on the application of the safeguards in ss. 15 and 16 of RIPA, in the sense that both apply to communications whether or not they are external.

126.4 Fourthly, as regards the examination of any intercepted material, the significant protection offered by s. 16(2) does not turn on the definition of external communications, but on the separate concept of a "*factor ... referable to an individual who is known to be for the time being in the British Islands*".

127. Each of these four points is addressed in greater detail below.

128. **First**, the definition of "*external communications*" is itself a sufficiently clear one, in the circumstances. All parties are agreed that (i) it draws a distinction between communications that are both sent and received within the British Islands, and communications that are not both sent and received within the British Islands; and (ii) the focus of the definition is upon the ultimate sender, and ultimate intended recipient, of the communication. Thus, for the purposes of determining whether a communication is internal or external it matters not that a particular communication may be handled either by persons or by servers en route, who are located outside the British Islands; what matters is only where the sender and intended recipient of the communication are based. See Mr Farr at §§129-130, and §98 of Privacy

International's skeleton. This position reflects what was stated by Lord Bassam during the passage of RIPA through Parliament (set out at §74 above).

129. Further, although the ways in which the internet may be used to communicate evolve and expand over time, the application of the definition remains foreseeable. Thus, where the ultimate recipient is *e.g.* a Google web server (in the case of a Google search), the status of the search query - as a communication - will depend on the location of the server. Further, when a communication in the form of a public post or other public message is placed on a web-based platform such as Facebook or Twitter, the communication will be external if the server in question (as the ultimate recipient) is outside the British Islands. By contrast, if such a platform is used to send what is in effect a private message to a particular individual recipient, then - as in the case of a telephone call, or an ordinary email - the status of the communication in question will depend on whether that recipient is within or outside the British Islands. (And the same analysis applies if the private message is sent to a group of individual recipients: as in the case of an ordinary email, the private message will be an internal communication if all recipients are within the British Islands). [*Farr §§133-137*][33]

130. That said, the nature of electronic communication over the internet means (and has always meant) that the factual analysis whether a particular communication is external or internal may in individual cases be a difficult one, which may only be possible to carry out with the benefit of hindsight. But that is not a question of any lack of clarity in RIPA or the Code: it reflects the nature of internet-based communications. For example, suppose that London-based A emails X at X's Gmail email address. The email will be sent to a Google server, in all probability outside the UK, where it will rest until X logs into his Gmail account to retrieve the email. At the point that X logs into his Google mail account, the transmission of the communication will be completed. If X is located within the British Islands at the time he logs into the Google mail account, the communication will be internal; if X is located outside the British Islands at that time, the communication will be external. Thus it cannot be known for certain whether the communication is in fact external or internal until X retrieves the email; and until X's location when he does so is analysed.

131. However, the Claimants wrongly assume that any such difficulties in applying the definition of "*external communication*" to a specific individual communication is relevant to the operation of the S. 8(4) Regime in relation to that communication. It is not:

[33] The implication of Liberty's contention that the Code should explain how the distinction between "*external*" and "*internal*" communications applies to various modern forms of internet use is that, each time a new form of internet communication is invented, or at least popularised, the Code would need to be amended, published in draft, and laid before both Houses of Parliament, in order specifically to explain how the distinction applied to the particular type of communication at issue. That would be both impractical and (for reasons explained below) pointless; and the "in accordance with the law" test under Art. 8 cannot conceivably impose such a requirement.

131.1 Whilst a s. 8(4) warrant in principle permits interception of what is (at the point of interception) a substantial volume of communications, it is necessary that the communications actually sought are "*external communications*" of a particular description, which must be set out in the warrant: see s. 8(4). Further, interception will be targeted at communications "*links*" (to use Lord Bassam's wording). However, the legislative framework expressly authorises the interception of internal communications not identified in the warrant, to the extent that this is necessary to obtain the "*external communications*" that are the subject of the warrant: see section 5(6)(a) RIPA; and (as Lord Bassam explained to Parliament, and given §70 above) it is in practice inevitable that, when intercepting material at the level of communications links, both "*internal*" and "*external*" communications will be intercepted.

131.2 Thus, the distinction between external and internal communications offers an important safeguard at a "macro" level, when it is determined what communications links should be targeted for interception under the S. 8(4) Regime. When deciding whether to sign a warrant under section 8(4) RIPA, the Secretary of State will – indeed must – select communications links for interception on the basis that they are likely to contain external communications of intelligence value, which it is proportionate to intercept. Moreover, interception operations under the S. 8(4) Regime are conducted in such a way that the interception of communications that are not external is kept to the minimum necessary to achieve the objective of intercepting wanted external communications [*Farr §154*]. However, that has nothing to do with the assessment whether, in any specific case, a particular internet-based communication is internal or external, applying the definition of in s. 20 of RIPA and the Code.

132. In short, how the definition of "*external communication*" applies to any particular electronic communication is immaterial to the foreseeability of its interception. This is the **second** point.

133. **Thirdly**, the safeguards in ss. 15 and 16 (as elaborated in the Code) apply to internal as much as to external communications, and thus the scope of application of these safeguards does not turn on the distinction between these two forms of communication.

134. **Fourthly**, it is the safeguard in s. 16(2) that affords significant protections for persons within the British Islands, and this provision does not turn on the definition of external communications, but on the separate concept of a "*factor ... referable to an individual who is known to be for the time being in the British Islands*".

135. For example, London-based person A undertakes a Google search. It appears to be common ground between the parties that such a search would in all probability be an external communication, because it would be a communication between a person in the British Islands and a Google server

probably located in the US. Nevertheless, irrespective of whether the communication was external or internal, it could lawfully be intercepted under a section 8(4) warrant which applied to the link carrying the communication, as explained above. However, it could not be examined by reference to a factor relating to A, unless the Secretary of State had certified under section 16(3) RIPA that such examination was necessary, by means of an express modification to the certificate accompanying the section 8(4) warrant.

136. Similarly, given s. 16(2), examining any one of the UK communications specified in each example in §101 of Privacy's skeleton without a warrant under section 8(1) RIPA or a certificate under section 16(3) RIPA would be unlawful, regardless of whether those communications were properly characterised as internal or external. In particular, there could be no conceivable factor which permitted the examination of communications of students in London, simply arranging a time for a night out, save one which related to the individuals in question. And without a warrant under section 8(1) RIPA or a certificate under section 16(3) RIPA, no such factor could ever be utilised.

Issue (vi): "In light of the factual premises at paragraphs (3) and (4) above, does the existence of the statutory regime as set out in paragraphs 102-178 of the [Original Open Response] amount in itself to an interference with the Claimants' Art. 10 rights, if any?"

137. §§56-59 are repeated *mutatis mutandis*.

Issue (vii): "In light of the factual premises at paragraphs (3) and (4) above, does the statutory regime as set out in paragraphs 102-178 of the [Original Open Response] satisfy the Art. 10(2) 'prescribed by law' requirement?"

138. **Yes** (see §147 of *Weber* and §§60-61 above).

139. The only respect in which the Claimants posit a different analysis under Art. 10 than under Art. 8 is that they say *"prior judicial authorisation is required before the state may seize and retain journalistic source material"*, citing *Sanoma Uitgevers BV v. The Netherlands* (2010) 51 EHRR 31: see Liberty's skeleton argument, §126.

140. A similar assertion was made to the Divisional Court in *Miranda v Secretary of State for the Home Department* [2014] HRLR 9, and was rejected: see *Miranda* at §§84-89 *per* Laws LJ.

141. The *Miranda* case concerned the stop and search at Heathrow Airport of the partner of a journalist (Glenn Greenwald) who had received stolen encrypted data from Edward Snowden, under the power in Sch. 7 of the Terrorism Act 2000. Thus, the search in *Miranda* was undertaken in the knowledge that the person searched was acting in support of Mr Greenwald's activities as a journalist, though the stolen data was not itself "*journalistic material*", or was "*journalistic*" only in the weakest sense (§72). Even in that context, the Court did not accept that prior judicial scrutiny was required before a search was

undertaken; and did not consider that such a general rule was laid down by the Strasbourg authorities. The Strasbourg cases which have concentrated on, and expressed in general terms the need for, prior judicial authorisation concern the targeted surveillance of journalists with a view to obtaining knowledge of their sources: see *Sanoma* and *Telegraaf Media Nederland Landelijke Media BV v. Netherlands* 34 BHRC 193. In those cases, the ECtHR found that there was a requirement for prior judicial authorisation precisely because the context was one in which journalists were targeted to obtain information, so that the general principles applicable to strategic monitoring, as stated in *Weber*, did not apply. See *e.g. Telegraaf Media* at §§96-97[34]. The Divisional Court in *Miranda* did not accept that the principles in those cases could simply be imported into any context in which Art. 10 was engaged, without sensitivity to the particular facts of the case. See Laws LJ at §88:

> *"Mr Kovats submits that the Strasbourg court has not developed an absolute rule of prior judicial scrutiny for cases involving state interference with journalistic freedom. In my judgment that is right. Although the court's reasoning is sometimes expressed in very general terms (see in particular [90] and [92] of Sanoma), in this area as in others its method and its practice is to concentrate on the facts of the particular case. And the Strasbourg court would itself acknowledge that the protections against excess of power by state agents, and the limitations which the law acknowledge that the protections against excess of power by state agents, and the limitations which the law imposes on the power they enjoy, vary greatly from state to state: such differences illustrate the importance of the well known doctrine of the margin of appreciation."* (Emphasis added.)

142. If in *Miranda,* the specific targeted search of a person known to be assisting a journalist did not require prior judicial authorisation, then *a fortiori* Art. 10 cannot require prior judicial authorisation for section 8(4) warrants, issued for the general purposes in section 5(3) RIPA (i.e. the interests of national security, the prevention or detection of serious crime, and the safeguarding of the economic well-being of the United Kingdom).

---

[34] *"96. In Weber and Saravia, the interference with the applicants' rights under Articles 8 and 10 consisted of the interception of telecommunications in order to identify and avert dangers in advance, or "strategic monitoring" as it is also called. The first applicant in that case being a journalist, the Court found that her right to protect her journalistic sources was in issue (loc. cit., §§ 144-45). However, the aim of strategic monitoring was not to identify journalists' sources. Generally the authorities would know only when examining the intercepted telecommunications, if at all, that a journalist's conversation had been monitored. Surveillance measures were, in particular, not directed at uncovering journalistic sources. The interference with freedom of expression by means of strategic monitoring could not, therefore, be characterised as particularly serious (loc. cit., § 151). Although admittedly there was no special provision for the protection of freedom of the press and, in particular, the non-disclosure of sources once the authorities had become aware that they had intercepted a journalist's conversation, the safeguards in place, which had been found to satisfy the requirements of Article 8, were considered adequate and effective for keeping the disclosure of journalistic sources to an unavoidable minimum (loc. cit., § 151).*
97. The present case is characterised precisely by the targeted surveillance of journalists in order to determine from whence they have obtained their information. It is therefore not possible to apply the same reasoning as in Weber and Saravia."

Issue (viii): **"Does the fact that any s. 8(4) warrants issued in respect of the alleged Tempora programme are neither issued by judges nor require the prior approval of judges give rise to a breach of the 'necessity' and 'in accordance with the law' requirements in Art. 8(2) and/or (if the answer to Issue (vi) is 'yes') Art. 10(2)?"**

143. 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) of RIPA) and to order the destruction of records obtained under them (s. 67(b)(i) of RIPA). (In addition, oversight is also provided by the Commissioner, who must hold or have held high judicial office.)

144. It is clear from §§167 and 169 of *Kennedy* that the Art. 8(2) "*necessity*" requirement does not require interception warrants to be issued by judges, or require prior judicial approval for such warrants. Nor does the "in accordance with the law" rubric require this. In particular, it is nowhere mentioned in §95 of *Weber*.

145. The answer to Issue (viii) is thus, **no**.

Issue (ix): **"Does the absence of a requirement that any s. 8(4) warrants issued in respect of the alleged Tempora programme target specific individuals or premises give rise to a breach of the 'necessity' and 'in accordance with the law' requirements in Art. 8(2) and/or (if the answer to Issue (vi) is 'yes') Art. 10(2)?"**

146. The answer to Issue (ix) is, **no**. The S. 8(4) regime sufficiently defines (1) the "*offences*" which may give rise to an interception order and (2) the categories of people liable to have their telephones tapped (see §§106-109 above). The point made in §72 above regarding the practical difficulties of investigating individuals and organisations abroad offers further significant support for this submission.

Issue (x): **"Are the 'necessity' and 'in accordance with the law' requirements in Art. 8(2) and/or (if the answer to Issue (v) is 'yes') Art. 10(2) breached because interception under the s. 8(4) regime issued in respect of the alleged Tempora programme may in principle involve (i) the interception (and subsequent recording) of communications and 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 communications and communications data 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?"**

147. **No**.

148. *Weber* is a complete answer to the Claimants' complaint in relation to Issue (x): this aspect of S. 8(4) Regime - which it shares with German strategic monitoring - does not in itself give rise to ECHR incompatibility (see §76.2 above). Nor could it be otherwise, as this aspect of both regimes is a practical necessity (see §§66-73 above).

Issue (xi): "Does the alleged Tempora programme and/or the s. 8(4) regime give rise to unlawful discrimination contrary to (i) Art. 14 of the ECHR (as as read with Art. 8 and/or Art. 10), (ii) Art. 6 TEU and the European Charter of Fundamental Rights and/or (iii) Art. 15(1) of Directive 2002/58/EC?"

149. The Respondents submit, **no**.

Is there any relevant difference in treatment?

150. The Claimants address the question whether the alleged "*Tempora*" programme and/or the S. 8(4) Regime give rise to unlawful discrimination at §§107-114 of Privacy International's skeleton argument, which are adopted by Liberty (see §132 of its skeleton argument); and Amnesty (see §§24-30 of its skeleton argument). The Claimants' case appears to be put in two ways: (i) by reference to the distinction between internal and external communications; and (ii) by reference to the safeguards under section 16 RIPA.

151. The distinction between the interception regime under s. 8(1) of RIPA and the S. 8(4) Regime is based upon the current location of persons whose communications are intercepted, not upon nationality or national origin. To take a pertinent example, the sort of communications covered by a s. 8(4) warrant of potential interest to the Intelligence Services would no doubt include the communications of British jihadists who had travelled to Syria or Iraq. The reason for distinguishing between external and internal communications in this way is the important practical difference between gathering intelligence on individuals and organisations within the UK, and gathering intelligence on individuals and organisations outside the jurisdiction, and the practical challenges inherent in obtaining external internet-based communications (see §§66-73 above).

152. The Claimants assert that the distinction between the two regimes is indirectly discriminatory on grounds of nationality and national origin, on the basis that British nationals are more likely to be present in the British Islands and *vice versa*. It is no doubt correct that in general British nationals are more likely to be present in the British Islands than non-British nationals. However, it does not follow that non-British nationals are any more likely to have their communications intercepted under the S. 8(4) Regime. "*External communications*" include those which are sent from outside the British Islands, to a recipient in the British Islands; or sent from within the British Islands, to a recipient outside the British Islands. Persons of non-British nationality are not necessarily any more likely than British nationals to have their communications intercepted under a regime which focuses upon certain types of "*external communication*"; particularly if, as the Claimants allege, the regime operates in relation to fibre optic cables within the British Islands. Indeed, it is difficult to see how the interception of communications under a s. 8(4) warrant even evinces discrimination between persons on the basis of location, because a person abroad is not necessarily any more likely to have their communications intercepted under such a warrant, than a person in the British Islands.

153. Thus, the distinction between internal and external communications in RIPA gives rises to no relevant discrimination whatsoever.

154. The sole respect in which persons may be treated differently by reason of location under the S. 8(4) Regime is that at the selection stage, limitations are imposed 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 (for example, by reference to a UK landline telephone number).

Justification

155. If and to the extent that the S. 8(4) Regime gives rise to any relevant indirect discrimination either under the ECHR or for the purposes of EU law[35], it is plainly justified.

156. The assessment of discrimination for the purposes of Art. 14 of the ECHR

35

entails an overall conclusion as to whether in the enjoyment of Convention rights there has been unfair and unjustifiable discrimination on the grounds of some personal characteristic. A distinction is to be drawn between grounds of discrimination under Art. 14 which *prima facie* appear to offend respect due to the individual (as in the case of sex or race), where severe scrutiny is called for; and those which merely require some rational justification, which include discrimination on grounds of residence: see *R (Carson and Reynolds) v. Secretary of State for Work and Pensions* [2006] 1 AC 173 (a case concerning the difference between the amount of state pension payable to persons resident in, and outside, Great Britain).

157. The legal test for justification of indirect discrimination under EU law is somewhat differently formulated – namely, whether the allegedly discriminatory provision, criterion or practice corresponds to a real need, and is appropriate and proportionate to that need – but it would be a curious outcome if the answer to the discrimination issue differed, depending upon whether an EU law or ECHR analysis is applied: and the Claimants themselves do not contend that the two analyses should lead to any different result.

158. In this case, the real need for the S. 8(4) Regime is that expressed by the Commissioner in his 2013 Annual Report at §6.5.51: there is no other reasonable means that would enable the Intelligence Agencies to have access to external communications which the Secretary of State judges it is necessary for them to obtain for a statutory purpose under the s.8(4) procedure. Moreover, the S. 8(4) Regime is appropriate and proportionate to that need, on the same basis. If a s. 8(1)-type regime were to be applied to the interception of external communications, the probability of obtaining any or any adequate intelligence about individuals and organisations operating outside the British Islands would be greatly reduced; and the only practical way in which the Government can ensure that it is able to obtain at least a fraction of the type of communications in which it needs for the statutory purposes is to provide for the interception of a large volume of communications, and the subsequent selection of a small fraction of those communications for examination by the use of relevant selectors [*Mr Farr §149*].

159. Further, it is plainly proportionate and justified to apply specific safeguards under s. 16 of RIPA to the selection of material for examination using factors referable to individuals who are known for the time being to be in the British Islands. Those safeguards reflect the fact that the Government has considerable legal and practical powers to obtain the communications of individuals known to be within the British Islands; those legal and practical powers make it feasible to name a person or set of premises to be targeted under a s. 8(1) warrant; and interception under a s. 8(4) warrant should not be used in order to circumvent the requirement for targeted interception under a s. 8(1) warrant.

160. The Claimants have no response to the obvious point that it is harder to investigate terrorism and crime abroad, save to assert that this cannot justify the allegedly "*less favourable*" treatment of countries "*where the UK has*

intelligence sharing relationships pursuant to the EU common foreign security policy or other arrangements". But in truth, that is no answer. There is an obvious difference between having one's own powers to investigate, and being reliant upon the goodwill of countries with which intelligence-sharing relationships exist.

161. In any event, the EU common foreign and security policy does not include an obligation to share intelligence, which would be contrary to Art. 346(1) TFEU[36]. To similar effect, cooperation between EU Member States and the EU body established to investigate, prevent and combat terrorism and serious and organised crime across the EU (Europol) is voluntary. There is no obligation imposed upon Member States to provide any intelligence to Europol, just as no such obligation exists between Member States themselves: see Art. 7 of Council Decision 2009/371 (the Council Decision of 6 April 2009 establishing Europol). The existence of voluntary intelligence-sharing relationships, under which information may be provided in part or not at all, is plainly miles away from being able to deploy the full powers of the State to investigate individuals located within the jurisdiction.

162. Finally, in response to the case law upon which the Claimants principally rely under this head:

162.1 The Claimants cite *Gaygusuz v. Austria* (1997) 23 EHRR 364 for the proposition that nationality discrimination requires "*very weighty*" justification. *Gaygusuz* concerned the refusal of emergency assistance to a Turkish national legally resident in Austria, on the sole basis that he was not Austrian. The ECtHR found that this contravened Art. 14 of the ECHR in conjunction with Art. 1 of the First Protocol, on the basis that *"very weighty reasons would have to be put forward before the Court could regard a difference in treatment based exclusively on the ground of nationality as compatible with the Convention"* (§42, emphasis added). *Gaygusuz* was, therefore, a case concerning direct nationality discrimination, where that was the only reason for a difference in treatment.

162.2 Here, by contrast, even on the Claimants' own case, any nationality discrimination is indirect only. Caution is necessary in applying the concept of indirect discrimination in the loosely-defined categories used by Art. 14 ECHR: see *e.g. Esfandiari v. Secretary of State for Work and Pensions* [2006] HRLR 26 at §§17-18; and there is no suggestion from *Gaygusuz* (or any other case) that indirect discrimination on nationality grounds would require "*very weighty*" justification. (Indeed, by definition, indirect discrimination on the basis of nationality could not be a difference in treatment based "*exclusively*" on nationality.)

162.3 *A v. Secretary of State for the Home Department* [2004] 2 AC 68 (the

[36] Art. 346(1) TFEU (ex Art. 296 TEC) states: "*The provisions of the Treaties shall not preclude the application of the following rules: (a) no Member State shall be obliged to supply information the disclosure of which it considers contrary to the essential interests of its security…*"

Belmarsh case) is not on point. That concerned direct discrimination on grounds of nationality between two sets of persons within the UK, both of whom presented the same threat (*i.e.* UK nationals suspected of terrorism, and non-UK nationals suspected of terrorism, only the latter being subject to detention without charge). For all the reasons already given above, that is not this case.

V: ISSUES OF LAW RELATING TO PROCEDURE

Issue (xii): "Are the Respondents obliged to depart from their [NCND] stance in relation to the alleged Tempora programme?"

163. In the Respondents' submission: **no.**

164. There is no context in which the NCND policy is more obviously important than the work of the Intelligence Services, for all the reasons given in Farr §§42-48. Secrecy about the Intelligence Services' capabilities and techniques, including the methods by which interception is obtained, is particularly important, for the reasons that Mr Farr gives. Moreover, denial (or indeed affirmation) of particular capabilities may also cause the indirect damage that, on a future occasion, it may be possible to infer information from a "*no comment*" response. As Mr Farr explains, that approach is particularly important in the context of leaks and other unauthorised disclosures of sensitive information [*Farr §46*].

165. The Claimants nevertheless take as a given that the Respondents are required specifically to justify any reliance on NCND in the context of this case in relation to the alleged "*Tempora*" programme, in the same way as they might justify a claim to public interest immunity in the civil courts; and assert that in the circumstances of this case, no such justification exists: see in particular Privacy International's skeleton argument, §115.

166. Those assertions assume, without argument, that the same position applies with regard to the use of NCND in the Tribunal, as applies to a claim of PII in cases in the civil courts: and moreover, cases in the civil courts which do not involve any closed procedure or closed evidence. That is plainly wrong. Further, the Claimants' contentions as to why a NCND stance in relation to the alleged "*Tempora*" programme is unjustified on the facts are also wrong.

167. **First**, for reasons set out more fully in answering the Claimants' allegations concerning disclosure (*i.e.* Issue (xiv) below), the Rules - as upheld in Strasbourg in *Kennedy* - do not require disclosure of information or documents between the parties. They prevent the Tribunal from disclosing to other parties information provided by one party to a case, without that party's consent; and prohibit the Tribunal from ordering such disclosure to be made in the absence of consent. See rule 6 of the Rules. For reasons explained in the Procedural Ruling, that "bright line" position is itself intended to, and does, preserve the NCND principle. Therefore, the Claimants' assertion that the Respondents are not entitled to rely on NCND simply ignores the legislative framework governing claims in the Tribunal.

168. This in itself is a complete answer to the Claimants' assertions about NCND.

169. In any event, and **secondly**, the Claimants' reliance on *R (Bancoult) v. Secretary of State for the Foreign and Commonwealth Office* [2014] Env LR 2 is misplaced. *Bancoult* concerned a single purported electronic cable emanating from the US embassy in London, obtained from the Wikileaks website, which purported to be a note of a meeting between British and US officials in 2009,

and which had been published by the *Guardian* newspaper. The claimants wished to rely on the contents of the cable as being a true record of the meeting. The Secretary of State neither confirmed nor denied the provenance of the cable. The question was whether the NCND principle precluded the cable being admitted in evidence, on the basis that it was indeed authentic. The Divisional Court did not require the Secretary of State himself to take a position on whether the document was authentic or not; but stated that if the only objection to the claimants themselves admitting it in evidence were the NCND principle, that objection would be overruled, inter alia because (i) the NCND principle did not bind the court; and (ii) the interests of justice would override the policy on the facts of the case. See §§26–28 of the Divisional Court's judgment, and §§72-73 of the judgment of the Court of Appeal on appeal ([2014] EWCA Civ 708).

170. Contrary to the Claimants' assertions, therefore, the *Bancoult* case is not authority for the proposition that a party must justify with specifics any use of NCND; nor for the proposition that NCND cannot apply to material in the public domain *"whose authenticity is not seriously disputed"* (assuming, which is not accepted, that that characterisation properly applies to any of the allegedly leaked material upon which the Claimants seek to rely). It establishes only that a policy of NCND cannot, if the interests of justice require otherwise, prevent another party to the case from adducing evidence that they already have.

171. It is also instructive to note the difference between the context in *Bancoult* and the present case. *Bancoult* concerned a purported diplomatic cable recording a conversation between US and UK officials, in the public domain before the case. It is unsurprising that the Courts concluded in those circumstances that its further disclosure in the proceedings could not be damaging. That is miles away from the present context, which concerns the alleged interception capabilities of the Intelligence Services.

172. **Thirdly**, the Claimants are wrong to assert that the material obtained by Edward Snowden makes any reliance on the principle of NCND in this case unjustified or inappropriate, still less (as they claim) *"absurd"*[37]. Various factual matters are relied upon in that respect at §115(f) of Privacy International's skeleton argument. None of them assists the Claimants. In particular:

    172.1 As to §115(f)(ii)-(iii), the Government has confirmed that Mr Snowden stole material from GCHQ's records, and that Mr Miranda was in possession of approximately 58,000 documents stolen from GCHQ when he was stopped by officials at Heathrow Airport on 18 August 2003. The Government has, however, never confirmed or denied the provenance of any documents placed in the public domain by Mr Snowden, or the truth or falsehood of any information contained within them[38].

[37] See Privacy International's skeleton argument, §115(f).
[38] See [*Farr §47*].

172.2 As to §115(f)(iv), the passage from the *Guardian* quoted by the Claimants shows that the Chairman of the Intelligence and Security Committee confirmed (as is well known) that fibre optic cables carrying a significant proportion of the world's communications pass close to the British coastline and could provide intelligence opportunities. He specifically did not confirm the existence of the alleged "*Tempora*" programme.

173. **Fourthly**, it is unclear from the Claimants' submissions on this issue exactly what they say the Respondents should now either confirm or deny. That stance in itself shows the very great danger of overriding the NCND principle.

174. Privacy International's skeleton argument states at §115(f) that "*the materials obtained by Edward Snowden and now published worldwide by various media outlets are a paradigm example of an absurd claim to NCND*". That is on the alleged basis that no protection to national security is needed, because "*any harm to national security has already been done by the original disclosure*": skeleton, §115(f)(v). Thus, the Claimants do not restrict arguments about the application of NCND to the confirmation or denial of the existence of the alleged "*Tempora*" programme itself. Rather, they imply that the Respondents should be required to confirm or deny all "*materials*" publicly disclosed by Edward Snowden, at least insofar as relevant to this case[39]. Indeed, on the Claimants' case, there is no logical distinction of principle to be made between confirmation and denial of the existence of the alleged "*Tempora*" programme, and confirmation and denial of any relevant material in documents publicly disclosed by Mr Snowden: both are matters to which the documents relate.

175. The fact that no such logical distinction can be made shows the absurdity of the Claimants' position. The NCND principle is likely to be most important precisely where (as here) one is dealing with an extremely serious leak. Also, it may readily be seen that if the Intelligence Agencies were required to confirm or deny the provenance, authenticity or contents of a mass of material placed in the public domain, it would have a catastrophic effect upon their ability to carry out their work.

Issue (xiii): "Does the Tribunal have power to direct that the government disclose information or evidence to the Claimants if the Tribunal is satisfied that the disclosure of the information or evidence would not be contrary to the public interest? If the answer is 'no', does the Tribunal have power to direct that the government make admissions, concessions or take any other steps as the Tribunal may direct, by analogy with CPR 80.25(7)?"

176. In the Respondents' submission both questions in Issue (xiii) should be answered, **no.**

Disclosure

177. The Claimants' arguments on disclosure are set out in Privacy International's

[39] See also §115(d) of the Privacy skeleton.

skeleton at §§116-122, and Amnesty's skeleton at §§32-33. Neither contends that rule 6 of the Rules does anything other than set out a "bright line" rule, under which the Tribunal has no power to direct the government to disclose information or evidence to the Claimants without its consent (see rule 6(5)); and no power to disclose information provided by any party to the case to any other party without consent, save in the circumstances set out in rule 6(4)[40].

178. The legal basis upon which the Claimants assert that the Tribunal does have power to order disclosure, notwithstanding the unambiguous prohibition on ordering disclosure in rule 6(5), is unclear. Amnesty's skeleton does not address this point, save to say that Amnesty "*reserves its right*" to challenge the ECtHR's ruling on the Tribunal's procedural powers in *Kennedy* before the ECtHR[41]. Privacy International's skeleton simply poses the rhetorical question *"why should [the Tribunal] not have the power to direct disclosure?"* without addressing the mandatory terms of the Rules.

179. The Tribunal gave detailed consideration to the validity of, and justification for, its procedural regime, including rule 6(5), in the Procedural Ruling. It held that:

179.1 Secret interception and surveillance operations, information and documents pose special problems for a tribunal established to consider and determine claims and complaints of violations of the ECHR rights of individuals. Those problems arise from the inescapable and incontrovertible fact that interception of communications and covert surveillance must, if they are to be used effectively, be and remain secret: §46.

179.2 A proper balance must be struck between the interests of complainants in maximum information and openness in the consideration and determination of their claims and complaints, including individuals' ECHR rights, and on the other hand, the interests of national security and other public interests served by the NCND policy: §§54-55.

179.3 RIPA and the Rules together represent a considered attempt by Parliament and the Secretary of State to strike that proper balance. They are the product of a discretionary judgment in the difficult area of what constitutes a necessary and proportionate response to the competing claims of ECHR rights and the NCND policy and other public interest considerations: §56.

179.4 In the circumstances, the departures from the adversarial model represented by the rules, including *inter alia* the lack of power to order disclosure, are within the rule-making power conferred upon the Secretary of State by section 69(1) RIPA, as limited by section

[40] *I.e.* as part of the information provided to a complainant under rule 13(2) on determination of the complaint in his favour, subject to the restrictions in rules 13(4) and (5).
[41] See §32 of Amnesty's skeleton argument.

69(6)(b)[42]. They provide for a fair trial within Art. 6 of the ECHR (assuming, contrary to the Respondents' position, it applies)[43]: see §181. They are also compatible with Arts. 8 and 10 of the ECHR, taking account of the exceptions for the public interest and national security in Arts. 8(2) and 10(2): see §182.

180. The Procedural Ruling was challenged before the ECtHR by Mr Kennedy (one of the Claimants in the proceedings that gave rise to the Procedural Ruling). The ECtHR unanimously rejected the challenge, stating at §187 of *Kennedy*, regarding disclosure:

> *"In respect of the rules limiting disclosure, the Court recalls that the entitlement to disclosure of relevant evidence is not an absolute right. The interests of national security or the need to keep secret methods of investigation of crime must be weighed against the general right to adversarial proceedings. The Court notes that the prohibition on disclosure set out in r. 6(2) admits of exceptions, set out in r. 6(3) and (4). Accordingly, the prohibition is not an absolute one. The Court further observes that documents submitted to the IPT in respect of a specific complaint, as well as details of any witnesses who have provided evidence, are likely to be highly sensitive, particularly when viewed in light of the Government's "neither confirm nor deny" policy. The Court agrees with the Government that, in the circumstances, it was not possible to disclose redacted documents or to appoint special advocates as these measures would not have achieved the aim of preserving the secrecy of whether any interception had taken place. It is also relevant that where the IPT finds in the applicant's favour, it can exercise its discretion to disclose such documents and information under r. 6(4)".*

181. *Contra* the suggestion in Privacy International's skeleton argument at §117, therefore, the ECtHR's findings were not on their face expressed in terms particular to Mr Kennedy alone; nor did they suggest that the bright line position on disclosure in the Rules would or might require any modification in other cases before the Tribunal.

182. In the circumstances, therefore, the restrictions on disclosure in rule 6 of the Rules are *intra vires* and should be upheld. In the Procedural Ruling, the Tribunal gave good reasons why the Rules were lawful and proportionate (including as respects disclosure); the ECtHR in *Kennedy* upheld the Procedural Ruling; and the Claimants have pointed to no deficiency in the Tribunal's reasoning. The mere fact that there has been significant experience of closed litigation in the ordinary courts and SIAC in the last decade does not alter that position. It should also be noted that the Supreme Court in *A v. B* [2010] 2 AC 1 considered the nature of the Tribunal's Rules, including

---

[42] By section 69(6)(b) RIPA, the Secretary of State is directed when making rules to have regard in particular to:

> *"... the need to secure that information is not disclosed to an extent, or in a manner, that is contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, the economic well-being of the United Kingdom or the continued discharge of the functions of any of the intelligence services."*

[43] Although the Tribunal found that Art. 6 applies, the ECtHR in *Kennedy* expressly left this issue open (see §179), in the light of the UK Government's submissions to the contrary (§§174-176).

restrictions on the disclosure of evidence, and did not suggest that they were either contrary to Convention rights, or prevented the proper determination of disputes in this particular context[44].

183. Moreover, the general position on disclosure does not prejudice the Claimants or prevent a fair trial of the issues in this case. The Respondents have conceded that the Claimants can properly challenge the legal regime for the interception of communications, on the basis that their communications might in principle have been intercepted. That is a challenge that the Claimants can, and do, make without needing to see material, the disclosure of which would damage national security. The Claimants' skeletons amply illustrate that the legal issues between the parties are ones which can properly be addressed, without further disclosure. Indeed, of all the Claimants, only Amnesty International asks at this stage for any specific further information by way of disclosure.

184. As to Amnesty's request for disclosure of the Respondents' internal arrangements under ss. 15 and 16 of RIPA (see Amnesty's skeleton argument, §33), Mr Farr has examined the safeguards in question, and explained in his skeleton that on the basis of that examination, the arrangements cannot safely be put into the public domain without undermining the effectiveness of interception methods, because they would explain in detail the manner in which interception is undertaken [*Farr §100*].

185. If and to the extent that the Claimants either (i) provide further grounds for challenging the Tribunal's procedural regime as regards disclosure, or (ii) make any further application for specific disclosure, the Respondents will address them at the appropriate time (including, if necessary, amplifying the legal submissions set out above).

Power to direct that the Government make admissions, etc.

186. Privacy International suggests in its skeleton argument at §§120-122 that, if the Tribunal considered particular material could properly be disclosed to the Claimants, and if the Respondents refused to disclose it, the Tribunal should direct that the Respondents are unable to rely upon it. This, it is said, is a solution that the Tribunal could adopt by analogy with CPR r. 82.14 (consideration of closed material application), in the exercise of its general power to determine its own procedure under s. 68(1) of RIPA.

187. That suggestion, and the analogy with CPR r. 82, are inapposite. CPR r. 82 is concerned with ordinary civil litigation, *i.e.* litigation involving usual duties of disclosure on either side. It applies where there has been a closed material application to court, and a special advocate has been appointed. In such a case, the court must consider whether to give permission to withhold "sensitive material" to the person who would otherwise be required to disclose it ("the relevant person"). If the court does not give such permission, then:

[44] See §14 of the judgment in *A v. B per* Lord Brown, with whom all the other members of the Court agreed.

187.1 In a departure from normal disclosure rules, the court cannot require the relevant person to serve it: see CPR r. 82.14(9)(a); but

187.2 If the relevant person does not serve it, they cannot rely upon it, or must make such concessions or take such other steps as the Court directs: see CPR r. 82.14(9)(b).

188. In short, under CPR r. 82.14, the premise for disentitling a party from relying upon particular sensitive material is the Court's conclusion that the material should properly be disclosed to the other side pursuant to disclosure duties.

189. That same premise, for obvious reasons, does not apply in a context where no disclosure duties exist as between the parties. Thus, if the Tribunal were to accede to the Claimants' suggestion, it would in practice be applying disclosure duties via the back door, in a context where no such duties exist (and indeed, where such duties are explicitly excluded by the Rules). That would be an inappropriate use of the Tribunal's general powers to regulate its own procedure, which is a power explicitly expressed to be "*Subject to any rules made under section 69*" (see s. 68(1) of RIPA).

190. As with the issue of disclosure, the Respondents will if necessary address this point in more detail, if and to the extent that the Claimants amplify their argument on the point, or assert that the Government should be put to its election in respect of any particular material.

Issue (xiv): "Does the Tribunal have power to request that the Attorney General appoint a Special Advocate to represent the interests of the Claimants in any closed hearings held under Rule 9(4)(b) of the Rules? If the answer is 'yes', when should the Tribunal exercise the power?"

191. In the Respondents' submission, and for the reasons that follow: the Tribunal **does** in principle have power to request the Attorney General to appoint a special advocate in the event of a closed hearing, subject to rule 6(1) of the Rules; but whether that power should be exercised should be considered in the particular context in which the issue arises, rather than in the abstract.

192. It will be necessary to hold at least one closed hearing under rule 9(4)(b) of the Rules in these cases. In particular, there is a need for a closed hearing before the Tribunal delivers its open judgment on the preliminary issues, in order to examine material which is relevant to the determination of those issues. At the very least, the Tribunal should have an opportunity to examine the Respondents' internal arrangements, guidance and policies insofar as they cannot safely be put into the public domain, for the purposes of Issues (i) and (iv). See §§26, 104-105 and 120 above.

193. Further, it may be necessary for the Tribunal to examine, for instance, the degree and scope of the Respondents' interception of external communications under the S. 8(4) Regime. For reasons already explained above (see §§8-13), the Respondents submit it is entirely unnecessary for the Tribunal to conduct a factual examination of those matters, in order to answer

the legal issues arising in the preliminary issues hearing. However, the Claimants make a number of factual assertions about the extent of interception under the S. 8(4) Regime which go far beyond the agreed factual premises. If and to the extent that the Tribunal were minded to take into account any of those assertions, it would be necessary for the Tribunal to go into closed session, in order for the Respondents to adduce evidence on the true position.

194. The Respondents submit that, for the purposes of any closed hearing, the Tribunal in principle has the power to seek the appointment of a Special Advocate under its general power to determine its own procedure under s. 68(1) of RIPA: but only if and to the extent that this was consistent with the Tribunal's duty under rule 6(1) of the Rules to carry out its functions in such a way as to secure that "*information is not disclosed to an extent, or in a manner, that is contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, the economic well-being of the United Kingdom or the continued discharge of the functions of any of the Intelligence services*". (The obvious danger with the appointment of a Special Advocate is that, unless they are appointed in every case, they allow a complainant to draw inferences about whether his communications have been intercepted.) Subject to that caveat, however, the power exists.

195. The Tribunal's general duty to exercise its functions concerning the disclosure of information in a manner that does not prejudice national security raises matters which are highly context-sensitive. The Respondents therefore consider it sensible to address the circumstances in which the Tribunal should exercise the power to request the appointment of a Special Advocate in due course and in the particular context in which the issue arises, rather than in the abstract.

JAMES EADIE QC
Blackstone Chambers

BEN HOOPER
JULIAN MILFORD
11KBW Chambers

3 July 2014