**Application No. 58170/13**

**IN THE EUROPEAN COURT OF HUMAN RIGHTS**
**BETWEEN:**

**BIG BROTHER WATCH and ors**

**Applicants**

**-and-**
**THE UNITED KINGDOM**

**Respondent**

**-and-**
**13 INTERVENING PARTIES**

**Intervenors**

**Application No. 24960/15**

**IN THE EUROPEAN COURT OF HUMAN RIGHTS**
**BETWEEN:**

**10 HUMAN RIGHTS ORGANISATIONS**

**Applicants**

**-and-**
**THE UNITED KINGDOM**

**Respondent**

**-and-**
**2 INTERVENING PARTIES**

**Intervenors**

**Application No. 62322/14**

**IN THE EUROPEAN COURT OF HUMAN RIGHTS**
**BETWEEN:**

**(1) BUREAU OF INVESTIGATIVE JOURNALISM**
**(2) ALICE ROSS**

**Applicants**

**-and-**

**THE UNITED KINGDOM**

**Respondent**

**-and-**
**5 INTERVENING PARTIES**

**Intervenors**

---

# OBSERVATIONS OF THE GOVERNMENT OF THE UNITED KINGDOM ON THE ADMISSIBILITY AND MERITS OF THE APPLICATION

---

**Foreign and Commonwealth Office**

**LONDON SW1A 2AH**

**29 September 2017**

*These Further, consolidated Observations set out a summary of the Government's case; address certain particularly material facts; set out oversight mechanisms within the Intelligence Sharing and s.8(4) Regimes (and, to the extent relevant, the s.22 Regime); and finally, answer the questions set out in the Court's letter of 10 July 2017 in turn. They do not repeat the relevant summaries of domestic law and practice in Part 2 of the Government's initial Observations in each case[1], or as regards the s.22 Regime, in the Government's BIJ Further Observations of 16 December 2016[2], but cross-refer to them where necessary.*

*These Further Observations use the same terms and acronyms used in the Government's Observations on Admissibility and the Merits in all 3 of the above cases, as explained in the Glossary to the Observations in each (for ease of access, the Glossary is at the end of these Further Observations).*

*References to Annexes are to the Annexes lodged with the Government's initial Observations. The Government has also inserted (in bold) document reference in the Agreed Core Bundle of Annexes (which contains only the most relevant parts of material documents). References to the Core Bundle are in the form "CB/y", where "y" is the tab number.*

*The following sets of submissions have been made by the parties:*

*(1) The Applicants' applications. These are referred to as "BBW Application", "10 HR Application", and "BIJ Application" respectively.*

*(2) An "Update Submission" from BBW, and "Submissions made in light of the Third IPT Judgment of 22 June 2015" from 10 HR.*

*(3) The Government's Observations. These are referred to as "BBW Observations", "10HR Observations", and "BIJ Observations" respectively.*

*(4) The Claimants' Observations in Reply. These are referred to as "BBW Obs in Reply", "10 HR Obs in Reply" and "BIJ Obs in Reply".*

*(5) The submissions of the various intervenors are referred to as "x Intervention", where "x" is the Intervenor's name.*

*(6) The Government's further observations of 16 December 2016. These are referred to as "BBW Further Observations of 16 December 2016" etc. In the case of BIJ and 10 HR, they incorporate a response to the submissions of the Intervenors in those cases.*

*(7) The Government's Response to the Intervenors' Submissions in BBW.*

## I INTRODUCTION

1. These cases are ones of the utmost importance to the UK. They are also of paramount importance to Council of Europe States who benefit from intelligence sharing arrangements with the United Kingdom or have similar legislative provisions governing the lawful interception and surveillance of communications. The information and intelligence obtained under the Intelligence Sharing and the s.8(4) Regimes are critical to the protection of the UK from national security threats - most particularly but not only the threat of terrorism. That is all the more so today, given the sophistication of terrorists and criminals in communicating over the internet in ways that avoid detection, whether that be through the use of encryption, the adoption of bespoke communications systems, or simply the volume of internet traffic in which they can now hide their communications. The internet is now used widely both to recruit terrorists, and to direct terrorist attacks, as well as by cyber criminals. Imposing additional fetters on interception or intelligence sharing would damage Member States' ability to safeguard national security and combat serious crime, at exactly the point when advances in communications technology have increased the threat from terrorists and criminals using the internet.

[1] See BBW Observations §§2.1-2.132, 10 HR Observations §§2.1-2.124, BIJ Observations §§80-202

[2] See BIJ Further Observations of 16 December 2016, §§41-56.

2. The seriousness of that threat, and its devastating consequences including the loss of innocent life, are underscored by recent events across the UK and Europe, including the attack on Westminster Bridge on 22 March 2017, the Manchester Arena bombing of 22 May 2017, the attack on London Bridge on 3 June 2017, the attacks in Barcelona and Cambrils on 17 August 2017, and the attack on London Underground on 15 September 2017.

3. Under the Convention scheme, it is properly for States to judge what systems are necessary to protect the general community from such threats. Of course, those systems are subject to the Court's scrutiny, because Convention rights are in play, and the systems must provide appropriate protection against abuse and arbitrariness by the State. However, it is important that, in assessing the detail of protection required, care is taken not to undermine the effectiveness of systems for obtaining life-saving intelligence that cannot be gathered in any other way. That is why the Court has consistently and rightly afforded States a broad margin of appreciation in this field.

4. The UK has a detailed set of controls and safeguards in place governing the activities under challenge. The Intelligence Sharing Regime and the s.8(4) Regime are contained in a combination of primary legislation, published Codes and internal arrangements (which for good operational reasons cannot be made public). The bedrock of these Regimes is the Convention concepts of necessity and proportionality. These fundamental principles govern all aspects of information and intelligence from obtaining it in the first place, to examining it, to handling, storing and disclosing it, and finally to its retention and deletion. The safeguards built into the Regimes include a comprehensive and effective system of oversight by Parliamentary Committee (the ISC), a specially appointed Commissioner (a former Lord Justice of Appeal), and a specialist Tribunal, the Investigatory Powers Tribunal ("IPT"). As appears below, both the ISC and the Commissioner have examined the Regimes in detail and have publicly reported. So too has the (former) independent person appointed to keep terrorism laws under review, David Anderson QC. His report also contains particularly useful material in the context of the present issues.

5. The IPT is of particular importance in this case. That is because in the Liberty proceedings[3] it conducted a conspicuously thorough and detailed examination of the very same issues that the Applicants now raise. It sat as a tribunal of five distinguished lawyers, including two High Court Judges. It held open hearings, initially over 5 full days. It considered a very large quantity of evidence and submissions produced by the parties. The Applicants were represented throughout by experienced teams of Leading and Junior Counsel. The IPT considered and applied the relevant Articles of the Convention (Articles 8, 10 and 14) and the Convention jurisprudence relating to them. It also conducted closed hearings. It did so because, unsurprisingly given the

[3] I.e. Proceedings in the IPT brought in 2013 by Liberty, Privacy, Amnesty International and various other civil liberties organisations, challenging the Intelligence Sharing and s.8(4) Regimes, in the same factual premises as are relevant to the present application. See the glossary.

context, there were some relevant aspects (relating to the facts concerning the Applicants, the nature of the safeguarding Regimes, and the Intelligence Services' capabilities) which could not be considered in open without damaging national security. At those hearings, and more generally, the IPT was assisted by Leading Counsel acting as Counsel to the Tribunal. That facilitated a thorough and rigorous examination of the relevant matters in closed – including specifically of the safeguards provided by internal arrangements in place to provide additional layers of protection surrounding any interferences with eg Article 8 rights. The IPT rightly concluded that the regimes were lawful and consistent with Articles 8, 10 and 14 ECHR[4].

6. The issues here are complicated by widespread misunderstanding and mischaracterisation of both the Intelligence Sharing and s.8(4) Regimes. It has been said – and is said by these Applicants - that the UK claims the right to intercept in bulk *"any communications that happen to traverse the UK"*[5], engages in "*mass surveillance*"[6]; and asserts an *"almost unfettered right"*[7] to obtain communications intercepted by other States. Those assertions are false.

   (1) The nature of both Regimes (and indeed of other aspects of the handling of bulk data by the Intelligence Services) has now been addressed in a number of detailed and independent analyses, drawing upon full access to information held by the Intelligence Services. Those are the Report from the Intelligence and Security Committee of Parliament ("ISC") of 17 March 2015 ("the ISC Report") at **CB/47**; annual reports by the Commissioner[8] for 2013, 2014 and 2015 (**CB/35-37**); *"A Question of Trust",* a report of June 2015 by the Investigatory Powers Review ("the Anderson Report", **CB/48**); and the Report of the Bulk Powers Review of August 2016 ("the Bulk Powers Review", **CB/50**). They have also, and importantly, been addressed in detail by the Investigatory Powers Tribunal ("IPT") in the domestic proceedings giving rise to the 10 HR Application (the "Liberty proceedings"); and, in relation to other related powers to obtain and examine bulk data, in a judgment dated 8 September 2017 ("the Privacy 2 judgment", **CB/21**).

   (2) All those sources have unanimously confirmed that the UK does not engage in "*mass surveillance*"; that the s.8(4) Regime does not permit generalised access to communications; that the selection of communications for examination is tightly and carefully controlled; and that the communications selected for examination under the Regime are those of the highest intelligence value (i.e. those of suspected criminals or

[4] In the case of the Intelligence Sharing Regime, that was with the benefit of further disclosure by the Intelligence Services of relevant internal safeguards during the proceedings, which was set out by the IPT in its judgments ("the Disclosure"), and which is now embodied in the Code.
[5] See e.g. 10 HR Obs in Reply, §2.
[6] See e.g. BIJ Application, §5
[7] See e.g. 10 HR Obs in Reply, §2
[8] I.e. the Interception of Communications Commissioner, appointed under s.57(1) RIPA: see the glossary to these Observations. The Interception of Communications Commissioner until 1 September 2017 was Sir Stanley Burnton, a former High Court Judge. From 1 September 2017, the office of the Interception of Communications Commissioner has been abolished, and the statutory functions of the Commissioner have been assumed by the Investigatory Powers Commissioner, appointed under section 227 of the Investigatory Powers Act 2017. The first Investigatory Powers Commissioner (Lord Justice Fulford, a Court of Appeal Judge) was appointed on 7 March 2017.

national security targets). As a result of the Liberty Proceedings, it has also now been publicly confirmed in the factual premises relevant to these applications (and is embodied in the Intelligence Sharing Regime) that the Intelligence Services will only ever seek intercepted communications from other States either where they concern a target who is already the subject of a warrant, or when the Secretary of State has personally considered and approved the request (no such request having been made to date). Such material is handled with exactly the same safeguards applied to material intercepted by the Intelligence Services themselves[9].

7. In short summary, the answer to the Court's questions is as follows:

(1) *Question 1*: the Big Brother Watch ("BBW") and Bureau of Investigative Journalism ("BIJ") Applicants are not victims in respect of the Intelligence Sharing Regime, and the BIJ Applicants are not victims in respect of the s.22 Regime either (where their complaint is based on a fundamental misunderstanding). See §§82-99 below, pp. 32-36.

(2) *Question 2*: the BBW and BIJ Applicants have failed to make use of the available and effective domestic remedy of a complaint to the IPT. See §§100-119 below, pp. 36-41.

(3) *Question 3*:
   (a) The Intelligence Sharing Regime is "in accordance with the law"/"prescribed by law" for the purposes of Articles 8/10. The law is accessible, and gives the individual adequate protection against arbitrary interference. No separate issue arises concerning necessity. See §§120-149 below, pp. 41-50.
   (b) The s.8(4) Regime is also "in accordance with the law"/"prescribed by law". Specifically, interception of communications under the regime satisfies all 6 criteria set out by the Court in this context in *Weber and Saravia v Germany* app. 54934/00 ("*Weber"*) at §95. The appropriate test for communications data is the more general one of adequate protection against arbitrary interference: the regime meets that test as concerns communications data, but if it were required to satisfy the *Weber* criteria, would in any event do so. As to the s.22 Regime, it has nothing to do with the interception of communications, and their resulting storage, and the BIJ Applicants' complaint that there is no system for the independent authorisation of the interception of communications data under s.22 RIPA is in any event wrong. See §§150-236 below, pp. 50-74.
   (c) The s.8(4) Regime satisfies the "necessity" test. See §§237-247 below, pp. 74-77.

(4) *Question 4*: the domestic proceedings brought by the 10 HR Applicants did not involve the determination of their civil rights and obligations under Article 6. See §§248-252 below, pp. 77-79.

[9] See in particular the content of the Disclosure from the Liberty Proceedings, now embodied in Chapter 12 of the Code: §2.23, 10 HR Observations.

(5) *Question 5*: in any event, the various complaints that the 10 HR Applicants make about the proceedings in the IPT are wholly baseless. The proceedings were plainly compliant with Article 6. See §§253-262 below, pp. 79-82.

(6) *Question 6*: the application of the safeguard in s.16 RIPA to persons known to be within the British Islands, and not to persons outwith the British Islands, does not constitute a relevant difference in treatment for the purposes of Article 14 ECHR. Moreover, even if it did constitute a relevant difference in treatment for the purposes of Article 14, it would plainly be justified. See §§263-271 below, pp. 82-85.

## II THE FACTS

### The Prism/Upstream Complaints

8. Both the 10 HR and BBW applications concern the Intelligence Services' alleged receipt of material obtained under Prism and Upstream[10]. Prism and Upstream are US surveillance programmes conducted under the authority of s.702 Foreign Intelligence Surveillance Act 1978 ("FISA")[11]. Prism and Upstream are targeted programmes, undertaken with the knowledge of the service provider and under Court-approved procedures, in accordance with extensive privacy protections for non-US nationals, including those embodied in Presidential Policy Directive 28 ("PPD 28") of January 2014, which requires US intelligence agencies to adopt data protection policies and procedures to the maximum extent consistent with national security, to be applied equally to all persons regardless of nationality. See the Government's BBW Observations at §§1.7-1.15[12].

9. 10 HR in particular now apparently seek to rely upon the UK Government's alleged receipt of information from the US, obtained by the US under the authority of EO 12333[13]. Any issue of information collected under EO 12333 is outside the scope of the Applications. In any event, just as under FISA, the collection of "foreign intelligence" under EO 12333 must be tied to the

[10] GCHQ has obtained information from the US that the US obtained via Prism. The Government neither confirms nor denies that either the Security Service or SIS has obtained information from the US collected via Prism, or that any of the Intelligence Services have obtained information collected under Upstream.

[11] See 10 HR Application §5, BBW Application §§20-25. FISA is at Annex 2.

[12] The mischaracterisation of Prism and Upstream as involving "bulk seizure, acquisition and storage" appears to result from a failure to distinguish between two different types of NSA programme: the collection of bulk telephone call records under section 215 of the USA Patriot Act - a programme which the Privacy and Civil Liberties Oversight Board ("PCLOB") recommended should cease in 2014 in its 2 July 2014 Report (see Annex 23), and which has ceased – and collection under FISA. That misunderstanding is widely shared, and has been repeated by various courts or other bodies in Council of Europe States. Nevertheless, it remains a clear misunderstanding.

[13] See 10 HR Obs in Reply §§64-68. The factual and legal position concerning the surveillance practices of the US at issue in these cases (i.e. under the authority of FISA), and indeed not at issue in these cases (i.e. under the authority of EO 12333) is set out in considerably more detail in the Government's Response to the Intervenors' Submissions in BBW, at §§59-67.

satisfaction of specific foreign intelligence requirements; must be carried out in accordance with the privacy protections afforded by PPD 28; and is subject to an oversight regime in the US governing the collection, retention and dissemination of information[14]. (For the avoidance of doubt, it is neither confirmed nor denied whether the Intelligence Services have obtained any intercepted material collected under the authority of EO 12333.)

10. In the Liberty proceedings, the Government explained the highly restricted circumstances in which relevant Intelligence Services sought intercepted communications (and associated communications data) from a foreign government, amounting to a set of internal rules. The rules were embodied in the IPT's judgment of 5 December 2014 ("the 5 December Judgment", **CB/14**) and now constitute Chapter 12 of the Code (**CB/33**). Chapter 12 states:

***"12 Rules for requesting and handling unanalysed intercepted communications from a foreign government***

***Application of this chapter***

*12.1 This chapter applies to those intercepting agencies that undertake interception under a section 8(4) warrant.*

***Requests for assistance other than in accordance with an international mutual assistance agreement***

*12.2 A request may only be made by the Intelligence Services to the government of a country or territory outside the United Kingdom for unanalysed intercepted communications (and associated communications data), otherwise than in accordance with an international mutual legal assistance agreement, if either:*

- *A relevant interception warrant under the Regulation of Investigatory Powers Act 2000 ("RIPA") has already been issued by the Secretary of State, the assistance of the foreign intelligence is necessary to obtain the communications at issue because they cannot be obtained under the relevant RIPA interception warrant and it is necessary and proportionate for the Intelligence Services to obtain those communications; or*

- *Making the request for the communications at issue in the absence of a relevant RIPA interception warrant does not amount to a deliberate circumvention of RIPA or otherwise frustrate the objectives of RIPA (for example, because it is not technically feasible to obtain the communications via RIPA interception), and it is necessary and proportionate for the Intelligence Services to obtain those communications.*

*12.3 A request falling within the second bullet of paragraph 12.2 may only be made in exceptional circumstances and must be considered and decided upon by the Secretary of State personally.*

*12.4 For these purposes a "relevant RIPA interception warrant" means one of the following: (i) a section 8(1) warrant in relation to the subject at issue; (ii) a section 8(4) warrant and an accompanying certificate which includes one or more "descriptions of intercepted material" (within the meaning of section 8(4)(b) of RIPA) covering the subject's communications, together with an appropriate section 16(3) modification (for individuals known to be within the British Islands); or (iii) a section 8(4) warrant and an accompanying certificate which includes one or more "descriptions of intercepted material" covering the subject's communications (for other individuals).*

***Safeguards applicable to the handling of unanalysed intercepted communications from a foreign***

[14] For further detail, see §67 of the Government's Response to the Third Party Intervenors in the BBW application.

***government***

*12.5 If a request falling within the second bullet of paragraph 12.2 is approved by the Secretary of State other than in relation to specific selectors, any communications obtained must not be examined by the intercepting agency according to any factors as are mentioned in section 16(2)(a) and (b) of RIPA unless the Secretary of State has personally considered and approved the examination of those communications by reference to such factors*[15].

*12.6 Where intercepted communications content or communications data are obtained by the intercepting agencies as set out in paragraph 12.2, or are otherwise received by them from the government of a country or territory outside the UK in circumstances where the material identifies itself as the product of an interception, (except in accordance with an international mutual assistance agreement), the communications content [fn whether analysed or unanalysed] and communications data [fn whether or not those data are associated with the content of communications] must be subject to the same internal rules and safeguards as the same categories of content or data, when they are obtained directly by the intercepting agencies as a result of interception under RIPA.*

*12.7 All requests in the absence of a relevant RIPA interception warrant to the government of a country or territory outside the UK for unanalysed intercepted communications (and associated communications data) will be notified to the Interception of Communications Commissioner."*

11. In sum, the effect of Chapter 12 of the Code is to confirm that, in the factual premises relevant to the Liberty proceedings (and therefore to these Applications), the only "raw intercept" requested by the Intelligence Services from any foreign government (including the USA) is either (i) intercepted material concerning targets who are already the subject of an interception warrant under Part I of RIPA, where that material cannot be obtained by the Intelligence Services themselves, and it is necessary and proportionate to obtain it; or (ii) in exceptional circumstances, and where necessary and appropriate, other material not covered by a RIPA interception warrant, provided that the request has been considered and decided upon by the Secretary of State for Foreign and Commonwealth Affairs. So far, no request falling within (ii) has ever been made. The Code also confirms that exactly the same internal safeguards governing use, disclosure, storage and destruction apply as a matter of substance to such material, as apply to similar material obtained through interception under Part I of RIPA.

12. Further, the Disclosure and Code, as set out above, and the findings of the ISC and Commissioner[16] also confirm that receipt of intelligence material from the US via Prism and Upstream (or indeed, receipt of any intelligence material whatsoever) is <u>not</u> (contrary the Applicants' allegations) used as a means of circumventing domestic constraints on interception,

---

[15] The following footnote appears within chapter 12 at this point: *"All other requests within paragraph 12.2 (whether with or without a relevant RIPA interception warrant) will be made for material to, from or about specific selectors (relating therefore to a specific individual or individuals). In these circumstances the Secretary of State will already therefore have approved the request for the specific individual(s) as set out in paragraph 12.2."*

[16] See the ISC's Statement of 17 July 2013 on its investigation into the allegation that GCHQ used Prism as a means of evading UK law (**CB/43**). See also the Commissioner's 2013 Annual Report at §§6.8.1-6.8.6 and the question and answer posed at the beginning of that section (**CB/35**):
*"8. Do British intelligence agencies receive from US agencies intercept material about British citizens which could not lawfully be acquired by intercept in the UK and vice versa and thereby circumvent domestic oversight regimes?*
*6.8.1 No. I have investigated the facts relevant to the allegations that have been published…"*

imposed via RIPA. That would be unlawful as a matter of basic domestic public law[17]. In short, the Applicants' factual assertions that the UK Intelligence Services may obtain data from the NSA in breach of domestic controls, or in circumstances where they could not lawfully obtain that data themselves, are wholly wrong.

**The complaints about the alleged Tempora operation**

13. All 3 Applications (BBW, 10 HR and BIJ) complain about the bulk interception of communications pursuant to the alleged "Tempora" interception operation. The Government can state (and has previously stated) that it intercepts communications in "bulk" – that is, at the level of communications cables – pursuant to the lawful authority of warrants under s.8(4) RIPA. Such interception is aimed at "external communications" (that is, communications sent or received outside the British Islands[18]). Its features are addressed by the Commissioner in his Annual Reports of 2013 (See Annex 11, **CB/35**) and 2014 (See Annex 12, **CB/36**); in the ISC Report §§49-77 (See Annex 13, **CB/47**); in the Anderson Report at chapter 10 (See Annex 14, **CB/48**); and in the Bulk Powers Review in Chapters 2, 5 and 9 and Annex 8 (**CB/50**). All have been able to investigate the interception capabilities of the Intelligence Services in detail, with the full cooperation of the Intelligence Services. Each has engaged with, or taken evidence from, many interested parties outside government, including some of the Applicants, for the purposes of drafting their Reports. The Government can confirm the factual accuracy of the Reports' accounts of the Intelligence Services' capabilities.

***The rationale for, and utility of, s.8(4) interception***

14. There are two fundamental reasons why it is necessary to intercept the contents of bearers for wanted external communications, both of which ultimately derive from the substantial practical difference between the Government's control over and powers to investigate individuals and organisations within the UK, and those that operate outside that jurisdiction[19] (see e.g. the Anderson Report at §10.22[20]):
    (1) Bulk interception is critical both for the discovery of threats, and for the discovery of targets who may be responsible for threats. When acquiring intelligence on activities overseas, the Intelligence Services do not have the same ability to identify targets or threats that they possess within the UK. For example, small items of intelligence (such as a suspect location) may be used to find links leading to a target overseas; but that can only be done, if the

[17] Specifically, it would be contrary to the principle of domestic public law set out by the House of Lords in *Padfield v Ministry of Agriculture, Fisheries and Food* [1968] AC 997 (Annex 31) for the Intelligence Services deliberately to circumvent safeguards and mechanisms in RIPA by asking a foreign intelligence agency to intercept communications instead. (The position would be different if, for example, it was not technically feasible for the UK to intercept those communications itself, or if such interception could not be carried out within the required timeframe.) See further §§2.21-2.22 of the Government's BBW Observations.

[18] See s.20 RIPA, §6.5 of the Code, and the Government's BBW Observations at §2.64.

[19] See Mr Farr's w/s at §§143-147 for a summary of those differences.

[20] See Annex 14, CB/48

Services have access to a substantial volume of communications through which to search for links.

(2) Even where the Intelligence Services know the identity of targets, their ability to understand what communications bearers those targets will use is limited, and their ability to access those bearers is not guaranteed. Subjects of interest are very likely to use a variety of different means of communication, and to change those means frequently. Moreover, electronic communications do not traverse the internet by routes that can necessarily be predicted. Communications will not take the geographically shortest route between sender and recipient, but the route that is most efficient, as determined by factors such as the cost of transmission, and the volume of traffic passing over particular parts of the internet at particular times of day. (That does not detract in the slightest from the fact that particular bearers may carry a high proportion of communications of a particular type[21]). So in order to obtain even a small proportion of the communications of known targets overseas, it is necessary for the Services to intercept a selection of bearers, and to scan the contents of all those bearers for the wanted communications.

15. In addition, there are technical reasons why it is necessary to intercept the entire contents of a bearer, in order to extract specific communications. The precise position is complex, and the technical details are sensitive, but the basic position is that communications 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. 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 as many of the packets associated with that communication as it can, and reassemble them[22].

16. Thus, if an intercepting agency needs (for example) to obtain communications sent to an individual (C) in Syria, whilst they are being transmitted over the internet, and has access to a given bearer down which such communications may travel, the intercepting agency will need to intercept all communications that are being transmitted over that bearer – at least for a short time – in order to discover whether any are intended for C. Further, since the packets associated with a given communication may take different routes to reach their common destination, it may be necessary to intercept all communications over more than one bearer to maximise the chance of identifying and obtaining the communications being sent to C. (So again, those bearers would be chosen that had the greatest chance of carrying the packets concerned.)

[21] This is why 10 HR is wrong to assert that the Government's assertion that it chooses bearers on the basis of the possible intelligence value of the traffic they carry is inconsistent with this description of how internet communications travel (see 10 HR Obs in Reply, §41). The route down which a particular email to or from Syria might travel is almost infinitely varied. However, specific bearers may nevertheless carry a high proportion of such emails. It is those upon which GCHQ would wish to focus, in order both to (i) intercept the communications of a particular target; or (ii) discover targets (for example) planning terrorist attacks from Syria.

[22] This position was very well understood at the time that RIPA was enacted: see the debate in the House of Lords for 15 July 2000, and the remarks of Lord Bassam (the responsible Government Minister) at Annex 26.

17. In summary, as Mr Farr stated at §149 (**CB/9**):

> *"Taking these considerations in the round, it will be apparent that the only practical way in which the Government can ensure that it is able to obtain at least a fraction of the type of communication in which it is interested is to provide for the interception of a large volume of communications, and the subsequent selection of a small fraction of those communications for examination by the application of relevant selectors."*

18. The Commissioner, the ISC Report, the Anderson Report and the Bulk Powers Review have all examined in detail the need for bulk interception of communications under s.8(4) RIPA (or equivalent powers) in the interests of the UK's national security. All have concluded there is no doubt that such a capability is valuable, because it meets intelligence needs which cannot be satisfied by any other reasonable means.

19. The Commissioner's Annual Report of 2013 (**CB/35**) asked at §6.4.49 whether there were other reasonable but less intrusive means of obtaining needed external communications, and concluded at §6.5.51[23]:

> *"I am satisfied that 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. This is a sensitive matter of considerable technical complexity which I have investigated in detail."*

20. Further, the Commissioner, having pointed out that there was a policy question whether the Intelligence Services should continue to be enabled to intercept external communications under s.8(4) RIPA, stated that he thought it "*obvious*" that, subject to sufficient safeguards, they should be: §6.5.56.

21. The ISC Report stated (see Annex 13, **CB/47**):

> *"It is essential that the Agencies can "discover" unknown threats. This is not just about identifying individuals who are responsible for threats, it is about finding those threats in the first place. Targeted techniques only work on "known" threats: bulk techniques (which themselves involve a degree of filtering and targeting) are essential if the Agencies are to discover those threats."* (§77(K))

On that basis, the ISC concluded that GCHQ's bulk interception capacity under s.8(4) RIPA was: *"a valuable capacity that should remain available to them",* and was used for *"complex problems relating directly to some of the UK's highest priority intelligence requirements"*: see §§81, 90.

22. The Anderson Report (**CB/48**) commented on the uses of bulk interception at §§7.22-7.27[24], noting the importance of bulk interception for target discovery; and observing that this did not

[23] See Annex 11

[24] See Annex 14

mean suspicion played no part in the selection of communications channels for interception, or in the design of searches conducted on intercepted material. Mr Anderson QC concluded that bulk access was (inter alia) the only means by which GCHQ could obtain the information it needed to develop effective responses to cyber threats[25]; that case studies left him in *"not the slightest doubt"* of the value of its role for protecting national security[26]; that there was no cause for him to recommend that collection in its current form should cease; and that its utility, particularly in fighting terrorism in the years since the London bombings of 2005, was clear to him[27].

23. The Anderson Report contains (at Annex 9) six "case study" examples of intelligence from the bulk interception of communications. The importance of those examples speaks for itself, not least in light of recent events in Paris and Brussels. In summary, they are:

    (1) The triggering of a manhunt for a known terrorist linked to previous attacks on UK citizens, at a time when other intelligence sources had gone cold, and the highlighting of links between the terrorist and extremists in the UK, ultimately enabling the successful disruption of a terrorist network ("Case Study 1").
    (2) The identification in 2010 of an airline worker with links to Al Qaida, who had offered to use his airport access to launch a terrorist attack from the UK, in circumstances where his identification would have been highly unlikely without access to bulk data ("Case Study 2").
    (3) The identification in 2010 of an Al Qaida plot to send out operatives to act as sleeper cells in Europe, and prepare waves of attacks. The operatives were identified by querying bulk data for specific patterns ("Case Study 3").
    (4) The discovery in 2011 of a network of extremists in the UK who had travelled to Pakistan for extremist training, and the discovery that they had made contact with Al Qaida ("Case Study 4").
    (5) Analysis of bulk data to track two men overseas who had used the world wide web to blackmail hundreds of children across the world. GCHQ was able to confirm their names and locations, leading to their arrest and jailing in their home country ("Case Study 5").
    (6) The discovery in 2014 of links between known ISIL extremists in Syria and a previously unidentified individual, preventing a bomb plot in mainland Europe which was materially ready to proceed. Bulk data was the trigger for the investigation ("Case Study 6").

---

[25] See §7.25 of the Anderson Report

[26] See §7.26 of the Anderson Report

[27] See §14.45 of the Anderson Report. At §14.44, Mr Anderson also had observations to make about a draft resolution from the Council of Europe's Committee on Legal Affairs and Human Rights, upon which the BBW Applicants heavily rely in their Update Submissions (see e.g. §16 of the Submissions). Mr Anderson QC adverted to *"contrasting reports"* from the Council of Europe on bulk data collection. He compared the findings and resolution of the Committee on Legal Affairs and Human Rights, which cast doubt on the efficacy of bulk interception, with a report of April 2015 from the European Commission for Democracy through Law. He observed that the notion that bulk interception is ineffective "*is contradicted by the detailed examples I have been shown at GCHQ*"'. He pointed out that aspects of the methodology upon which the Committee's findings were made "*seem debatable*", and failed to take into account "*the potential of safeguards, regulation and oversight*". He commented that the April 2015 report was drafted "*in considerably more moderate (and on the basis of what I have seen realistic) terms*".

24. Quite aside from the direct threats to life set out above, bulk interception is also the only way in which the Intelligence Services can realistically discover cyber threats: a danger which potentially affects almost every person in the UK using a computer. The scale of the issue is one to which Mr Anderson QC adverted, when he pointed out that over a 2-week period bulk access had enabled GCHQ to discover 96 separate cyber-attack campaigns. The internet is an intrinsically insecure environment, with billions of computers constantly running millions of complex programmes. PwC's 2015 Information security breaches survey (See Annex 56) reported that 90% of large organisations and 74% of small businesses had a security breach in the period covered by the report; the average cost of the worst serious breach ranged from £1.46m to £3.14m for large organisations, and £75,000 to £311,000 for small businesses.

25. Finally, the utility of bulk interception carried out by GCHQ under the s.8(4) Regime was considered in still further detail in the Bulk Powers Review at Chapter 5, on the basis of an intensive review of *"a great deal of closed material concerning the value of bulk interception"* (see §5.2). Mr Anderson QC set out detailed reasons in Chapter 5 why intelligence obtained under the s.8(4) Regime will or may not be obtainable in any other way, and stated in conclusion:

> *"5.53 This Review has given me the opportunity to revisit my earlier conclusion [in the Anderson Report] with the help of Review team members skilled respectively in technology, in complex investigations and in the interrogation of intelligence personnel, and on the basis of considerably more evidence: notably, a variety of well-evidenced case studies, internal documentation and the statistic that almost half of GCHQ's intelligence reporting is based on data obtained under bulk interception warrants.*
>
> *5.54 My opinion can be summarised as follows:*
>
> *(a) the bulk interception power has proven itself to be of vital utility across the range of GCHQ's operational areas, including counter-terrorism in the UK and abroad, cyber-defence, child sexual exploitation, organised crime and the support of military operations.*
>
> *(b) The power has been of value in target discovery but also in target development, the triaging of leads and as a basis for disruptive action. It has played an important part, for example, in the prevention of bomb attacks, the rescue of a hostage and the thwarting of numerous cyber-attacks.*
>
> *(c) While the principal value of the power lies in the collection of secondary data, the collection and analysis of content have also been of very great utility, particularly in assessing the intentions and plans of targets, sometimes in crucial situations.*
>
> *(d) The various suggested alternatives, alone or in combination, may be useful in individual cases but fall short of matching the results that can be achieved using the bulk interception capability. They may also be slower, more expensive, more intrusive or riskier to life."*

26. The Bulk Powers Review (**CB/50**) emphasised in particular the importance of bulk interception for target discovery, i.e. finding previously unknown threats. See in particular:
    (1) §5.3 of the Bulk Powers Review:

> "*<u>Bulk interception is essential because the security and intelligence agencies frequently have only small fragments of intelligence or early, unformed, leads about people overseas who pose a threat to the UK</u>. Equally, terrorists, criminals and hostile foreign intelligence services are increasingly sophisticated at evading detection by traditional means. Just as importantly, due to the nature of the*

*global internet, the route a particular communication will travel is hugely unpredictable. Combined, this means that sometimes the data acquired via bulk interception is the only way the security and intelligence agencies can gain insight into particular areas and threats…"* (Emphasis added)

(2) Annex 7 to the Bulk Powers Review, which sets out GCHQ's "Statement of Utility of Bulk Capabilities", supplied to the Review in July 2016, stating inter alia:

*"GCHQ would not be able to identify those who wish us harm without bulk powers. Terrorists, child abusers, drug traffickers, weapons smugglers and other serious criminals choose to hide in the darkest places on the internet. GCHQ uses its bulk powers to access the internet at scale so as then to dissect it with surgical precision.*

*By drawing out fragments of intelligence from each of the bulk powers and fitting them together like a jigsaw, GCHQ is able to find new threats to the UK and our way of life; to track those who seek to do us harm, and to help disrupt them.*

- ***Bulk Interception:*** *Interception provides valuable information that allows us to discover new threats. It also provides unique intelligence about the plans and intentions of current targets – through interception of the content of their communications. Communications data obtained through bulk interception is also crucial to GCHQ's ability to protect the UK against cyber-attack from our most savvy adversaries and to track them down in the vast morass of the internet."*

27. Annex 8 to the Bulk Powers Review contains 13 "case studies", illustrating the use of and need for bulk interception, and providing context and a factual underpinning for the conclusions in chapter 5. Four of those case studies were summarised (albeit in slightly less detail) in the Anderson Report, as to which see the Government's BBW Observations, §1.36. Those are the identification in 2011 of a network of extremists in UK, on the basis of an email address obtained through complex queries of bulk data; the identification and monitoring of a senior Al Qaida leader and his network through interrogation of bulk data, leading to the arrest and conviction of a UK-based terrorist planning to use airport access to launch an attack; the arrest and jailing of men using the world wide web to blackmail children; and the discovery in 2014 of links between known ISIL extremists in Syria and a previously unidentified individual, preventing a bomb plot in mainland Europe. The other nine are summarised below. As with the examples in the Anderson Report, their importance speaks for itself:

(1) In 2015, GCHQ used communications data obtained under bulk interception warrants to search for new phones used by individuals known to be plotting terrorist acts in the UK. Following the identification of a new phone number, GCHQ eventually identified an operational cell, and its analysis revealed that the cell had almost completed the final stages of a terrorist attack. The police were able to disrupt the plot in the final hours before the planned attack. Without access to bulk data, GCHQ would not have been able to complete this work at all. See Case Study A8/1.

(2) Following terrorist attacks in France, GCHQ provided support to MI5 and European partners in identifying targets and prioritising leads. GCHQ triaged around 1,600 international leads (in the form of telephone numbers, email addresses or other identifiers) in the days following the attacks. It was necessary quickly to determine whether there was any further attack planning, and to identify leads that should be prioritised for further investigation. Without bulk data, that triage work would have taken much longer – potentially many months – and

would have led to GCHQ obtaining an incomplete picture, providing only limited assurance that further attack planning had been identified or ruled out: Case Study A8/3.

(3) During the UK's Afghanistan campaign, analysis of data obtained through bulk interception enabled GCHQ to locate and monitor an armed group that had taken hostages captive. Within 72 hours of the kidnapping, the hostages were located. They were subsequently rescued. There was no likely alternative method to bulk interception through which the hostage-takers could have been identified and located, or their intentions revealed: Case Study A8/6.

(4) During the UK's Afghanistan campaign, GCHQ used analysis of data obtained under bulk interception warrants to identify mobile devices in the area of Camp Bastion, the main base for UK forces. Analysis flowing from that data revealed that extensive attacks on Camp Bastion were being planned by multiple insurgents. The information led to several such attacks being disrupted. There was no practical means to obtain the information on a targeted basis. See Case Study A8/7.

(5) GCHQ used bulk interception to identify sophisticated malware placed on a nationally important UK computer network by an overseas-based criminal gang. Further analysis of the bulk data identified the infrastructure used to control the malware. The information obtained by GCHQ eventually led to the arrest of the gang. This is by no means an isolated incident: GCHQ deals with over 200 cyber incidents a month. See Case Study A8/8.

(6) In 2016, a European media company suffered a major, destructive cyber-attack. The analysis of bulk data permitted GCHQ (i) to link this attack to other attacks, and to explain what had happened; and (ii) to identify a possible imminent threat to the UK from the same cyber-attackers. As a result, GCHQ was able to protect government networks, and warn media organisations so that they were able to protect their own networks. GCHQ would have been unable to achieve the same outcome without the use of bulk powers: Case Study A8/9.

(7) Bulk data has given GCHQ significant insight into the nature and scale of online child sexual exploitation activity. In April 2016 alone, GCHQ identified several hundred thousand separate IP addresses worldwide being used to access indecent images of children through the use of bulk data. Further analysis can then lead (for example) to targeting those whose online behaviour suggests they pose the greatest risk of committing physical or sexual assaults against children: see Case Study A8/10.

(8) Between November 2014 and November 2015, GCHQ's analysis of data obtained under bulk interception warrants led to significant disruption of cocaine trafficking, involving the seizure of cocaine with a street value of around £1.1 billion. The traffickers could not have been identified, tracked, and disrupted without the use of bulk interception: Case Study A8/12.

(9) In early 2015, GCHQ's analysis of data obtained under bulk interception warrants was able to identify the multiple communications methods used by the principal members of an organised crime group involved in human trafficking into the UK. The information enabled investigations which eventually resulted in the release of a group of trafficked women, and the individual concerned was subsequently arrested: Case Study A8/13.

28. Much of the aim of interception pursuant to the s.8(4) Regime is not to search for the communications of identified targets. Rather, it is to ascertain, via the application of complex searches, who should be a target in the first place ("target discovery"). It is to identify who are

the individuals, groups and organisations outside the UK that pose a threat to the UK, because without such a power the Intelligence Services would be unable to tell who they were. Well over half of the examples referred to in the previous paragraph concern the discovery of previously unknown targets through the use of a bulk interception capability, instead of (or in addition to) the tracking of known targets. See §§27(2), (3), (4), (5), (7), (8), (9) above. See also the following:

(1) The Bulk Powers Review at §5.3:

> "*Bulk interception is essential because the security and intelligence agencies frequently have only small fragments of intelligence or early, unformed, leads about people overseas who pose a threat to the UK. Equally, terrorists, criminals and hostile foreign intelligence services are increasingly sophisticated at evading detection by traditional means. Just as importantly, due to the nature of the global internet, the route a particular communication will travel is hugely unpredictable. Combined, this means that sometimes the data acquired via bulk interception is the only way the security and intelligence agencies can gain insight into particular areas and threats…"* (Emphasis added)

(2) Annex 7 to the Bulk Powers Review, which sets out GCHQ's "Statement of Utility of Bulk Capabilities", supplied to the Review in July 2016, stating inter alia:

> *"GCHQ would not be able to identify those who wish us harm without bulk powers. Terrorists, child abusers, drug traffickers, weapons smugglers and other serious criminals choose to hide in the darkest places on the internet. GCHQ uses its bulk powers to access the internet at scale so as then to dissect it with surgical precision.*
> *By drawing out fragments of intelligence from each of the bulk powers and fitting them together like a jigsaw, GCHQ is able to find new threats to the UK and our way of life; to track those who seek to do us harm, and to help disrupt them.*
>
> - ***Bulk Interception:*** *Interception provides valuable information that allows us to discover new threats. It also provides unique intelligence about the plans and intentions of current targets – through interception of the content of their communications. Communications data obtained through bulk interception is also crucial to GCHQ's ability to protect the UK against cyber-attack from our most savvy adversaries and to track them down in the vast morass of the internet."* (Emphasis added)

(3) The ISC's Report[28] at vii on page 3 ("Key Findings"), under the heading "Why do the Agencies intercept communications?"

> *"(b) As a "discovery" or "intelligence-gathering", tool. The Agencies can use targeted interception only after they have discovered that a threat exists. They require separate capabilities to uncover those threats in the first place, so that they can generate leads and obtain the information they need to then target those individuals…"*

29. The overall conclusion on the bulk acquisition of communications data reached in the Bulk Powers Review by David Anderson QC was set out in §6.47:

> "*I have concluded that:*

[28] Annex 13, CB/47

*(a) Bulk acquisition has been demonstrated to be crucial in a variety of fields, including counter-terrorism, counter-espionage and counter-proliferation. The case studies provide examples in which bulk acquisition has contributed significantly to the disruption of terrorist operations and, through that disruption, almost certainly the saving of lives.*
*(b) Bulk acquisition is valuable as a basis for action in the face of imminent threat, though its principal utility lies in swift target identification and development.*
*(c) The SIAs' ability to interrogate the aggregated data obtained through bulk acquisition cannot, at least with currently available technology, be matched through the use of data obtained by targeted means.*
*(d) Even where alternatives might be available, they are frequently more intrusive than the use of bulk acquisition.*"

30. More generally, the Privacy 2 judgment from the IPT (**CB/21**) has recently reconsidered both the need for bulk data capabilities, the actual manner of their operation (rather than often ill-informed and inaccurate assertions or assumptions) and the nature of the attendant safeguards (the impact of an imposition of the sort of safeguards considered in eg the CJEU's judgment in *Watson*[29] is considered below). At this stage, the following matters appearing from the judgment are to be noted.

(1) The IPT recorded that there were two facts which were uncontroversial and in any event established by the evidence. They were first that "the use of Bulk Data capabilities is critical to the ability of the SIAs to secure national security" (or as they put it later at §17: "*The finding of this Tribunal is that these capabilities are essential to the protection of the national security of the United Kingdom*"); and secondly, that "a fundamental feature of many of the SIAs' techniques of interrogating Bulk Data is that they are non-targeted, i.e. not directed at specific targets" (§9(i) and (ii)) – that being because, as the ISC put it "*It is essential that the Agencies can "discover" unknown threats. This is not just about identifying individuals who are responsible for threats, it is about finding those threats in the first place. Targeted techniques only work on "known" threats: Bulk techniques (which themselves involve a degree of filtering and targeting) are essential if the Agencies are to discover those threats.*"
(2) The IPT noted the particular importance of the Anderson report as being "*that it was conducted by a team of independent persons…, with considerable expertise in the use of secret intelligence, and with the necessary security clearance to obtain access to secret documents, in order to analyse a number of actual case studies, to judge the effect and utility of the bulk powers. The reviewers were not only able to review documents, but also to question intelligence officers to ascertain whether the case being made for the use of those powers was justified*" (§11).
(3) The IPT specifically agreed with the overall conclusion reached by David Anderson QC at §6.47, commenting: "*Those findings fully support the evidence given in this case by the Respondents that the use of bulk communications data is of critical value to the intelligence agencies, and is of particular value in identifying potential threats by persons who are not the target of any investigation. These datasets need to be as comprehensive as possible if they are to be effective. The use of these datasets is very different from, for example, their*

[29] Joined Cases *Tele2 Sverige C-203/15* and *Watson & ors C-698/15*, 21 December 2016

*use in an investigation of a criminal offence by police, in which case the police may well have an identified suspect who can be made the subject of a targeted investigation. The Respondents' witnesses speak persuasively of developing fragmentary intelligence, of enriching 'seed' information, of following patterns and anomalies, and of the need for the haystack in order to find the needle"*(§14).

(4) The IPT took the view that there was "*considerable force"* in the submissions made to them that "*a. The use of bulk acquisition and automated processing produces less intrusion than other means of obtaining information. b. The balance between privacy and the protection of public safety is not and should not be equal. Privacy is important and abuse must be avoided by proper safeguards, but protection of the public is preeminent. c. The existence of intrusion as a result of electronic searching must not be overstated, and indeed must be understood to be minimal. d. There is no evidence of inhibition upon, or discouragement of, the lawful use of telephonic communication. Indeed the reverse is the case. e. Requirements or safeguards are necessary but must not, as the Respondents put it, eviscerate or cripple public protection, particularly at a time of high threat*" (§50).

***How bulk interception under the s.8(4) Regime works***

31. It is of fundamental importance to the questions raised by these Applications to understand how bulk interception under the s.8(4) Regime operates. In particular, it is critical to appreciate that although, for technical reasons, it is necessary to intercept the entire contents of a fibre optic cable (or "bearer") in order to obtain any intercepted communications from it at all, there is no possibility whatsoever of any such communications being viewed by an analyst, unless and until they are selected for examination; that selection (and any ensuing examination) are very carefully controlled; and that the overwhelming bulk of communications flowing over that bearer can never be so selected, but will (and must) be discarded.

32. Bulk interception under the s.8(4) Regime involves three stages[30]:

(1) Collection.
At this stage, GCHQ selects bearers to access on the basis of the likely intelligence value of the communications they carry. GCHQ only processes a fraction of the bearers it has the ability to access. It will select that fraction on the basis of those bearers most likely to be carrying external communications of intelligence value. GCHQ will do this by regular surveys of the contents of bearers: for example, a particular cable might carry a high proportion of communications to or from Syria. In practical terms, "accessing" means making a copy of the communications flowing down the bearer.

(2) Filtering
GCHQ's processing systems automatically discard in near-real time a significant proportion of the communications on the targeted bearers, on the basis that it comprises the traffic of a type least likely to be of intelligence value.

[30] See in particular Chapter 2 of the Bulk Powers Review at §§2.15-2.20

(3) Selection for examination

The remaining communications are then subjected to the application of queries, both simple and complex, to draw out communications of intelligence value which may potentially be viewed by an analyst. Queries may be either "simple" (in that they require the application of a single "strong selector", such as a telephone number or email address), or "complex" (in that they combine a number of criteria, which may include weaker selectors, but which in combination aim to reduce the odds of a false positive). Communications which match the relevant selectors are retained for possible examination; all other communications are discarded.

33. At the "selection for examination" stage, the "strong selector" (i.e. "simple query") process is applied against all the bearers that GCHQ has chosen to access. As observed by the ISC: *"while this process has been described as bulk interception because of the numbers of communications it covers, it is nevertheless targeted since the selectors used relate to individual targets"*. In short, this aims to extract the communications of specified targets, albeit that it is necessary to intercept the entire contents of a bearer for a very short time, to enable this to be done. See the ISC Report, §§61-63. The "complex query" process is applied against a far smaller number of bearers. Those bearers are not chosen at random: GCHQ focuses its resources on those most likely to carry items of intelligence value. The process entails 2 stages: (i) the initial application of a set of processing rules, designed to discard material least likely to be of value; and (ii) the application of complex queries to the material so selected, in order to draw out items which relate to GCHQ's statutory functions, and the selection of which meets tests of necessity and proportionality. Those searches generate an index. Only items contained in the index can potentially be examined by analysts. All other communications must be discarded. See the ISC Report, §§67-73, and the Bulk Powers Review at §2.19.

34. The selection of communications for examination, whether via "strong selectors" or "complex queries", and any ensuing examination, is very carefully controlled. Automated systems are used (and by §7.14 of the Code[31], must be used) to effect the selection for examination, save where a limited number of specifically authorised staff access intercepted material for the specific purpose of checking whether it falls within the Secretary of State's certificate, or to check whether the selection methodology remains up-to-date and effective. Any analysts who then examine selected material will be specially authorised to do so, and receive mandatory regular training, including training on the requirements of necessity and proportionality (see Code, §7.15). They will be vetted. Before they examine the material, they must create a record setting out why access to the material is required, consistent with the Secretary of State's certificate and the requirements of RIPA; and why it is proportionate (including considerations of any circumstances likely to give rise to a degree of collateral infringement of privacy). Unless such a record has been created, GCHQ's systems do not permit access to material.

35. Only a fraction of those communications selected for possible examination by either of the processing systems set out above is ever in fact looked at by an analyst.

[31] See Annex 10, CB/33.

(1) In relation to communications obtained via the use of "simple selectors", an automated "triage" process is applied, to determine which will be of most use. This triage process means that the vast majority of the items collected in this way are never looked at by an analyst, even where they are known to relate to specific targets.
(2) In relation to communications obtained via the application of complex search terms, items are presented to analysts as a series of indexes in tabular form showing the result of searches. To access the full content of any item, the analyst has to decide to open the specific item of interest based on the information in the index, using their judgment and experience. In simple terms, this can be considered as an exercise similar to that conducted when deciding what search results to examine, from a list compiled by a search engine such as Bing or Google. The remainder of the potentially relevant items are never opened or read by analysts.

36. The factual position set out above is consistent with the conclusion of the Commissioner in his Annual Report for 2013 at §6.7.5:

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

37. The above considerations amply illustrate why it is simply wrong for the Applicants to suggest that a selector might be used to *"store and analyse the reading habits of the population",* or *"identify everyone who had read a particular book"*[32]. The selection stage would not permit the use of such a selector; nor could an analyst provide the required justification for examining material on this basis. It might be the case that a complex query selected communications for examination on the basis of accessing known extremist literature, where that was combined (say) with being in a particular location such as northern Iraq; or using a particular computer language associated with terrorism. But using such a complex search to identify a target is not only doing exactly what GCHQ's systems are designed for, but is of vital utility to the United Kingdom's national security.

38. Interception under a s. 8(4) warrant is directed at "external communications" of a description to which the warrant relates: that is, at communications sent or received outside the British Islands (see s.20 RIPA). But the fact that electronic communications may take any route to reach their destination inevitably means that a proportion of communications flowing over a bearer between the UK and another State will consist of "internal communications": i.e., communications between persons located in the British Islands.

39. When conducting interception under a s.8(4) warrant, knowledge of the way in which communications are routed over the internet is combined with regular surveys of internet traffic

[32] See 10 HR Obs in Reply, §§43-44.

to identify those bearers that are most likely to contain external communications that will meet the descriptions of material certified by the Secretary of State as necessary to intercept. While this approach may lead to the interception of some communications that are not external, s.8(4) operations are conducted in a way that keeps this to the minimum necessary to achieve the objective of intercepting wanted external communications: see Farr §154 (**CB/9**). Mr Farr gave various examples of communications which he regarded as "internal", and those which he regarded as "external" at Farr §§134-138. For example, he indicated that a "Google" search was in effect a communication between the person conducting the search, and Google's index of web pages, hosted on its servers; and that because those servers were in general based in the US, such a search might well be an external communication. The Applicants have criticised those examples as "expansive" and/or "arbitrary" in their Update Submissions[33]. That criticism is misplaced; but more importantly, the Applicants have neglected to mention Mr Farr's observation that the question whether a particular communication is internal or external is entirely distinct from (and irrelevant to) the question whether it can lawfully be selected for examination: see Farr §§139-141, 157-158. (That point is expanded upon further below, in answer to the Applicants' criticism of the definition of "external communications" see §§221-228 below).

**Proceedings in the IPT**

40. Liberty, Privacy, Amnesty International and other civil liberties organisations brought claims in the IPT in 2013 ("the Liberty proceedings"), which similarly concerned the lawfulness of the UK's intelligence sharing and s.8(4) regimes, in the context of allegations about Prism, Upstream, and the alleged Tempora operation. Therefore, while there are some differences between the allegations made in these Applications and those made in the Liberty Proceedings, the IPT had the opportunity in the Liberty Proceedings to consider and rule upon most of the issues that the Applicants now raise.

41. The IPT, which consisted in this case of five experienced members, including two High Court judges, held a 5-day open hearing in July 2014 at which issues of law were considered on assumed facts. It also:

    (1) Considered additional legal issues in a series of further open hearings;
    (2) Considered the internal policies and practices of the relevant Intelligence Services in further open and (to the extent that such policies and practices could not be publicly disclosed for reasons of national security) closed hearings; and
    (3) Considered evidence which could not be disclosed for reasons of national security in closed hearings. Such evidence concerned the operation of the Intelligence Sharing and s.8(4) Regimes; and matters of proportionality (both of the regime and of the interception of the claimants' communications (if any)).

[33] See BBW's Update Submissions, §§50-57.

42. Throughout the hearings, the claimants were represented by teams of counsel, and the IPT had the benefit of assistance from experienced Counsel to the Tribunal ("CTT"). CTT (Martin Chamberlain QC) was appointed on the specific basis that he would make submissions from the perspective of the claimants' interests, and that his role at any closed hearing would be similar to that performed by a Special Advocate in closed proceedings, so that he would thoroughly test any closed evidence presented by the defendants (including any justification for selecting the claimants' communications for examination, if material)[34]. Following those hearings, the IPT issued a series of open judgments, as set out below.

***Judgment of 5 December 2014***

43. In its judgment of 5 December 2014 ("The 5 December Judgment", **CB/14**) the IPT considered a series of questions concerning the lawfulness of the Intelligence Sharing Regime and the s.8(4) Regime. The questions were answered on the agreed factual premises that the claimants' communications (i) might in principle have been obtained via Prism or Upstream, and provided to the Intelligence Services; and (ii) might in principle have been intercepted and examined under the s.8(4) Regime[35]. The IPT adopted the shorthand "Prism issue" and "s.8(4) issue" for the matters arising under each head.

44. The IPT found as follows in relation to the **Prism** issue:

(1) The Prism issue engaged Article 8 ECHR, and required that any interference with the claimants' communications be "in accordance with the law" on the basis of the principles in *Malone v UK* and *Bykov v Russia* (app. 4378/02, GC, 10 March 2009). See judgment, §§37-38.
(2) In light of the Disclosure, the respondents' arrangements for the purposes of the Prism issue were in accordance with the law under Articles 8 and 10 ECHR. There were adequate arrangements "below the waterline", which were sufficiently signposted by virtue of (i) the applicable statutory framework; (ii) statements of the ISC and Commissioner concerning the Prism issue (as to which, see footnote 16 above), and (iii) the Disclosure itself: judgment, §55.
(3) The only remaining issue was whether there was a breach of Article 8 ECHR prior to the judgment, because the Disclosure had not been made. That issue would be considered further, in light of submissions from the parties: judgment, §154.

45. In relation to the **s.8(4)** issue:

(1) The s.8(4) system, leaving aside the effect of s.16 RIPA, sufficiently complied with the *Weber* criteria[36], and was in accordance with the law. Moreover, the ECtHR's own

[34] See §10 of the 5 December Judgment, and the Note from CTT and response from the IPT at **CB/12-13**

[35] I.e. pursuant to bulk interception under a s.8(4) warrant

[36] I.e. the six criteria set out at §95 of *Weber and Saravia v Germany*

conclusions on the oversight mechanisms under RIPA in *Kennedy* endorsed that conclusion. See judgment, §§117-140.

(2) Any indirect discrimination within the s.8(4) system by virtue of a distinction in the protections afforded to persons within the UK and outside the UK was proportionate and justified: judgment, §§141-148.

(3) No distinction fell to be made between the analysis for the purposes of Article 8 ECHR and Article 10 ECHR: judgment, §§149-152.

46. The IPT stated in conclusion at §§158-159 of the judgment:

> *"158. Technology in the surveillance field appears to be advancing at break-neck speed. This has given rise to submissions that the UK legislation has failed to keep abreast of the consequences of these advances, and is ill fitted to do so; and that in any event Parliament has failed to provide safeguards adequate to meet those developments. All this inevitably creates considerable tension between the competing interests, and the "Snowden revelations" in particular have led to the impression voiced in some quarters that the law in some way permits the Intelligence Services carte blanche to do what they will. We are satisfied that this is not the case.*
>
> *159. We can be satisfied that, as addressed and disclosed in this judgment, in this sensitive field of national security, in relation to the areas addressed in this case, the law gives individuals an adequate indication as to the circumstances in which and the conditions upon which the Intelligence Services are entitled to resort to interception, or make use of intercept."*

***Judgment of 6 February 2015***

47. In a judgment of 6 February 2015 ("the 6 February Judgment", **CB/15**), the IPT considered the outstanding issue in §154 of its 5 December Judgment, namely whether prior to the Disclosure the Intelligence Sharing regime was in accordance with the law. It held that it was not, because without the Disclosure the internal arrangements for handling of material received via Prism/Upstream (if any) were inadequately signposted. However, it declared that in light of the Disclosure the regime was now in accordance with the law.

***Judgment of 22 June 2015***

48. The IPT's judgment of 22 June 2015 ("the 22 June Judgment", **CB/16**) concerned the issue whether there had in fact been unlawful conduct in relation to any of the claimants' communications under either of the Intelligence Sharing or the s.8(4) Regimes. In determining that issue, the IPT considered proportionality both as it arose specifically in relation to the claimants' communications, and as it arose in relation to the s.8(4) Regime as a whole (i.e. what the IPT described as "systemic proportionality"): see judgment, §3.

49. The IPT concluded that there had been unlawful conduct in relation to two of the claimants, whose communications had been intercepted and selected for examination under the s.8(4) Regime: namely, the Legal Resources Centre and Amnesty International. In each case, the unlawful conduct in question was "technical", in that it had caused the claimants no prejudice (so that a declaration constituted just satisfaction):

(1) Email communications associated with Amnesty International[37] had been lawfully and proportionately intercepted and selected for examination by GCHQ. They had in error been retained for longer than permitted under GCHQ's internal policies. So their retention was not "in accordance with the law". However, they were not accessed after the expiry of the relevant time limit: see judgment, §14.

(2) Communications from an email address associated with the Legal Resource Centre had been lawfully and proportionately intercepted, and proportionately selected for examination. However, GCHQ's internal procedures for selection had not been followed. Accordingly, their selection for examination was not "in accordance with the law". However, no use had been made of any intercepted material, nor any record retained: see judgment, §15.

50. Notwithstanding the "technical" nature of the breaches, the IPT made clear that it took them very seriously, stating at §18:

> *"The Tribunal is concerned that steps should be taken to ensure that neither of the breaches of procedure referred to in this Determination occurs again. For the avoidance of doubt, the Tribunal makes it clear that it will be making a closed report to the Prime Minister pursuant to s.68(5) of RIPA."*

51. The Applicants have suggested that these findings show that *"the dragnet of bulk intercept includes routine and automated storage of the communications of human rights advocates"*[38]. In fact, they show the opposite. The IPT did not explain (for national security reasons) precisely who the email communications in question were from or to; nor who was the actual target of any selection for examination. But if the communications had been selected for examination simply because they were associated with Amnesty International or the Legal Resource Centre, that would have been obviously disproportionate; and the IPT would have so stated. Instead, the IPT expressly found that the selection for examination of these particular emails was lawful and proportionate – and thus, necessary for a purpose set out in the Secretary of State's certificate.

## Oversight of the intelligence sharing and s.8(4) regimes

52. There are two principal oversight mechanisms common to both the Intelligence Sharing and s.8(4) Regimes: the ISC and the IPT (and the same mechanisms also apply to any issue concerning an authorisation for obtaining communications data under s.22 RIPA).

### *The ISC*

[37] The references to the Egyptian Initiative for Personal Rights in the 22 June Judgment should be references to Amnesty International. See the IPT's letter of 2 July 2015. The 22 June Judgment did not reveal whether or not the particular email address or addresses associated with the claimants had themselves been the target of the interception, or whether they had simply been in communication with the target of the interception.

[38] See 10 HR Obs in Reply, §47.

53. SIS and GCHQ are responsible to the Foreign Secretary,[39] who in turn is responsible to Parliament. Similarly, the Security Service is responsible to the Home Secretary, who in turn is responsible to Parliament. In addition, the ISC plays an important part in overseeing the activities of the Intelligence Services. It is the principal method by which Parliamentary scrutiny is brought to bear on those activities.

54. The ISC was established by s. 10 of the ISA. As from 25 June 2013, the statutory framework for the ISC is set out in ss. 1-4 of and Sch. 1 to the JSA. It consists of nine members, drawn from both the House of Commons and the House of Lords, none of whom can be Ministers, and who are appointed by the House from which they are drawn. The current chair is The Rt Hon Dominic Grieve QC MP, a former Attorney General. The Government has no power to remove a member of the ISC. The ISC may examine the expenditure, administration, policy and operations of each of the Intelligence Services: s. 2(1). Subject to certain limited exceptions, the Government (including each of the Intelligence Services) must make available to the ISC information that it requests in the exercise of its functions. See §§4-5 of Sch. 1 to the JSA. In practice, and where it is necessary to do so for the purposes of overseeing the full range of the activities of the Intelligence Services, the ISC is provided with all such sensitive information as it needs: see Farr §71.

55. The ISC operates within the "ring of secrecy" which is protected by the OSA. It may therefore consider classified information, and in practice takes oral evidence from the Foreign and Home Secretaries, the Director-General of the Security Service, the Chief of SIS and the Director of GCHQ, and their staff. The ISC meets at least weekly whilst Parliament is sitting. The ISC may also hold open evidence sessions: see Farr §66.

56. The ISC must make an annual report to Parliament on the discharge of its functions (s. 3(1) of the JSA), and may make such other reports to Parliament as it considers appropriate (s. 3(2) of the JSA). The ISC sets its own work programme: it may issue reports more frequently than annually and has in practice done so for the purposes of addressing specific issues relating to the work of the Intelligence Services. The ISC also monitors the Government to ensure that any recommendations it makes in its reports are acted upon: see Farr §70, Annex 3.

57. The ISC has investigated in detail interception issues raised by these cases. The Snowden allegations led it to conclude that an in-depth inquiry into the Intelligence Services' intrusive capabilities was required, and it carried out that review with the benefit of information about the "*full range of Agency capabilities*"[40], setting out its conclusions in the ISC Report.

***The IPT***

[39] The Chief of the Intelligence Service and the Director of GCHQ must each make an annual report on, respectively, the work of SIS and GCHQ to the Prime Minister and the Secretary of State (see ss. 2(4) and 4(4) of the ISA). An analogous duty is imposed on the Director-General of the Security Service (see s. 2(4) of the SSA).
[40] See §12 of the ISC Report, Annex 13, CB/47.

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

59. The IPT's jurisdiction is broad. It has exclusive jurisdiction to consider claims under s. 7(1)(a) HRA brought against any of the Intelligence Services or any other person in respect of any conduct, or proposed conduct, by or on behalf of any of the Intelligence Services (i.e., claims for breach of the ECHR, including of rights under Articles 6, 8, 10 and 14 ECHR). It has jurisdiction to consider and determine any complaints by a person who is aggrieved by any conduct by or on behalf of any of the Intelligence Services which he believes to have taken place in relation to him, to any of his property, to any communications sent by or to him, or intended for him, or to his use of any telecommunications service or system. It also has jurisdiction to consider challenges by any person to conduct which has taken place with the authority, or purported authority, of an interception warrant; or conduct which should not appropriately have taken place without an interception warrant or without proper consideration having been given to obtaining one. See s.65 RIPA[41].

60. The IPT may thus entertain <u>any</u> ECHR claim or public law complaint about the operation or alleged operation of the Intelligence Sharing or s.8(4) Regimes (or indeed, if that were relevant, any complaint about the operation of the s.22 regime for the acquisition and disclosure of communications data). In doing so, the IPT holds public hearings wherever possible (i.e. where they do not risk disclosure of sensitive information), including hearings on hypothetical facts, and will issue public judgments following such hearings. It can also consider matters which for reasons of national security cannot be disclosed into "open", and does so by holding closed hearings, often with the assistance of Counsel to the Tribunal (as in the Liberty proceedings). When it makes a determination in favour of a claimant, it must provide the complainant with a summary of that determination, including any findings of fact.

61. Under s. 67(7) RIPA, the IPT may (in addition to awarding compensation or making any other order that it thinks fit) make an order quashing or cancelling any warrant and an order requiring the destruction of any records of information which has been obtained in exercise of any power conferred by a warrant, or which is held by a public authority in relation to any person. That includes, obviously, any information obtained under either the Intelligence Sharing or s.8(4) Regimes.

62. Further, where a claimant / complainant succeeds before the IPT and the IPT's determination relates to any act or omission by or on behalf of the Secretary of State, or to conduct for which any warrant was issued by the Secretary of State, the IPT is by s. 68(5) RIPA required to make a report of their findings to the Prime Minister.

63. S. 68(6) RIPA imposes a broad duty of disclosure to the IPT on, among others, every person

[41] The precise details of the statutory regime, and the nature of the IPT's jurisdiction, are set out in the Government's BBW Observations at §§2.39-2.45 and 2.127-2.132.

holding office under the Crown (thus, including officers of the Intelligence Services). Such persons must disclose *"all such documents and information as the Tribunal may require"*. Sections 57 and 59 RIPA also require the Commissioner and Intelligence Services Commissioner to give the IPT any assistance it requires. As held by Lord Brown in *R(A) v Director of Establishments of Security Service* [2010] 2 AC 1[42] at §14:

> *"…There are…a number of counterbalancing provisions both in RIPA and the [IPT Rules] to ensure that proceedings before the IPT are (in the words of section 69(6)(a) RIPA) "properly heard and considered". Section 68(6) imposes on all who hold office under the Crown and on many others too the widest possible duties to provide information and documents to the IPT as they may require. Public interest immunity could never be invoked against such a requirement. So too sections 57(3) and 59(3) impose respectively upon the Interception of Communications Commissioner and the Intelligence Services Commissioner duties to give the IPT "all such assistance" as it may require. Section 18(1)(c) disapplies the otherwise highly restrictive effect of section 17 (regarding the existence and use of intercept material) in the case of IPT proceedings. And rule 11(1) [of the IPT Rules] allows the IPT to "receive evidence in any form, and [to] receive evidence that would not be admissible in a court of law." All these provisions in their various ways are designed to ensure that, even in the most sensitive of intelligence cases, disputes can be properly determined. None of them are available in the courts."*

64. Any person, regardless of nationality, may bring a claim in the IPT[43]. As the Court observed in *Kennedy v UK* (app. 26839/05) at [167], *"any person who suspects that his communications have been or are being intercepted may apply to the IPT".* As a result, the IPT is perhaps one of the most far-reaching systems of judicial oversight over intelligence matters in the world.

65. The Applicants have contended on the basis of a recent case in the IPT (*Human Rights Watch Inc and ors v Secretary of State for the Foreign & Commonwealth Office* [2016] UKIPTrib 15 165-CH, **CB/56**) that the IPT has *"abandoned"* this approach to jurisdiction[44]. That is wrong. It has reaffirmed it. The *Human Rights Watch* case concerned complaints by 10 complainants, arising out of a worldwide campaign by Privacy International to encourage anyone to apply to the IPT alleging illegality by GCHQ[45]. The worldwide campaign led to 663 applications. The first 10 were listed for hearing. The IPT was persuaded that 6 of those 10 had provided sufficient information to show they had grounds for some kind of belief that their communications were intercepted, so that their complaints should be entertained; but that others who had provided no grounds whatsoever for any suspicion of interception did not have standing[46]. So, as stated in

---

[42] See Annex 57

[43] However the IPT may refuse to entertain a claim that is frivolous or vexatious (see s. 67(4)). There is also a 1 year limitation period (subject to extension where that is "equitable"): see s. 67(5) of RIPA and s. 7(5) of the HRA. Any claims under the HRA would also have to satisfy the Article 1 ECHR jurisdiction threshold.

[44] See 10 HR Obs in Reply, §97.

[45] Privacy International's invitation, on the back of the Liberty proceedings, was as follows: *"Because of our recent victory against GCHQ in court, now anyone in the world – yes, ANYONE, including you – can try to find out if GCHQ illegally had access to information about you from the NSA. Make your claim using one of the options below, and send it to the IPT to try to find out if GCHQ illegally spied on you."*

[46] See §45 of the judgment. The IPT stated: *"We are a tribunal dedicated towards an efficient disposal of claims by those who have grounds of some kind for belief that their communications are being intercepted, as opposed to being a*

*Kennedy,* the test is suspicion, not proof, of interception: albeit the suspicion must have some basis other than random conjecture. The IPT observed that this was wholly consistent with the requirements of the "victim" test under the ECHR (as set out in *Zakharov v Russia* app. no. 47143/06). The test applied by the IPT is certainly no less generous than that in *Zakharov.* If anything, it is more generous.

66. The IPT's effectiveness, its wide experience in dealing with claims concerning surveillance or other activities of the Intelligence Services, its readiness to make findings of unlawfulness where appropriate, and the Government's implementation of changes following such findings, are all exemplified in a number of recent cases. For instance, quite apart from the Liberty proceedings, in the last 2 years:

    (1) The IPT has determined the lawfulness and compatibility with the ECHR of the regime regulating computer network exploitation activities by the Intelligence Services, making use of CTT and open and closed hearings (as in the Liberty proceedings): *Privacy International and Greennet v SSFCO and GCHQ* UKIPT 14/85/CH (Annex 42).
    (2) The IPT has determined a series of complaints that the regime for the interception of legally privileged communications was not in accordance with the ECHR. It gave a determination in favour of one complainant and ordered the destruction of various records: *Belhadj ors ors v The Security Service and ors* UKIPT/13/132-9/H (Annex 58). As a result of the IPT's findings in those proceedings, the Government has amended the applicable legal regime (by altering and strengthening the Code, as in the Liberty proceedings).
    (3) The IPT has determined a complaint against the Metropolitan Police by News Group Newspapers concerning the lawfulness of four authorisations issued under s.22 RIPA, finding one to be unlawful, and making a declaration (and quashing the authorisation) accordingly: *News Group Newspapers Limited v Metropolitan Police Commissioner* UKIPT/14/176/H (Annex 45).
    (4) The IPT has determined the lawfulness of the regime regulating the Intelligence Services' obtaining of bulk personal datasets and bulk communications data from CSPs, finding that the regimes were unlawful prior to March and November 2015 respectively, but lawful thereafter: *Privacy International v SSFCO and ors* UKIPT/15/110/CH.

***The Commissioner***

67. The Commissioner (and now, the Investigatory Powers Commissioner, who has taken over the Commissioner's functions from 1 September 2017) provides an important means by which the exercise by the Intelligence Services of their powers may be subject to effective oversight whilst maintaining appropriate levels of confidentiality regarding those activities. The Commissioner must hold or have held high judicial office, so as to ensure that he is appropriately independent from the Government (s.57(5) RIPA[47]). The Commissioner (quite properly) is independent from

*recipient of possibly hundreds of thousands of applications from people who have no such basis other than the mere existence of the legislation."*

[47] S.57 and 58 RIPA have been repealed (subject to specified savings) with effect from 1 September 2017, when the Investigatory Powers Commissioner took over the statutory functions of the Commissioner. The statutory framework

Government and the Intelligence Services: see e.g. the 2013 Annual Report at §§6.3.1-6.3.4 (Annex 11, **CB/35**).

68. The Commissioner's statutory functions include keeping under review the exercise of the powers and duties of the Secretary of State and the Intelligence Services under Chapter I Part I RIPA, including safeguards on handling intercepted material; and the exercise and performance of powers and duties conferred or imposed by Chapter II Part I RIPA (i.e. the acquisition of communications data): ss. 57(2)(a), (c), (d) RIPA. He is by statute to be provided with sufficient technical facilities and staff properly to carry out those functions: s. 57(7).

69. A duty is imposed on, among other persons, every person holding office under the Crown to disclose and provide to the Commissioner all such documents and information as he may require for the purpose of enabling him to carry out his functions: s. 58(1).

70. In practice, the Commissioner (via an inspection team of 2-3 people) has visited each Intelligence Service and the main Departments of State twice a year, for 3 days on each occasion (see 2015 Annual Report, §6.48. Inspections are thorough and detailed. A typical inspection of an interception agency, to scrutinise the key areas covered by interception under Chapter I Part I RIPA, will include the following (see 2015 Annual Report, §6.43, **CB/37**):

> *"- a review of the action points or recommendations from the previous inspection and their implementation;*
> - *an evaluation of the systems in place for the interception of communications to ensure they are sufficient for the purposes of RIPA and that all relevant records have been kept;*
> - *examination of selected interception applications to assess whether they were necessary in the first instance and then whether the requests met the necessity and proportionality requirements;*
> - *interviews with case officers, analysts and/or linguists from selected operations to assess whether the interception and justifications for acquiring all the material were proportionate;*
> - *examination of any urgent oral approvals to check the process was justified and used appropriately;*
> - *A review of those cases where communications subject to legal privilege or otherwise confidential information (e.g. confidential journalistic, or confidential medical) have been intercepted and retained, and any cases where a lawyer is the subject of an investigation;*
> - *An investigation of the procedures in place for the retention, storage and destruction of intercepted material and related communications data;*
> - *A review of the errors reported, including checking that the measures put in place to prevent recurrence are sufficient."*

71. Representative samples of warrantry paperwork are scrutinised (2015 Annual Report §6.49, **CB/37**) including the paperwork for s. 8(4) warrants [Farr §91]. The total number of warrants specifically examined equated in 2015 to three quarters of the extant warrants at the end of the year, and three eighths of new warrants issued in 2015 (2015 Annual Report, §6.50). The examination process is a 3-stage one, as the 2015 Report explains at §6.49:

---

governing the functions and powers of the Investigatory Powers Commissioner is contained in the Investigatory Powers Act 2016.

*" - First, to achieve a representative sample we select warrants across different crime types and national security threats. In addition we focus on those of particular interest or sensitivity, for example those which give rise to an unusual degree of collateral intrusion, those which have been extant for a considerable period (in order to assess the continued necessity for interception), those which were approved orally, those which resulted in the interception of legal or otherwise confidential communications, and so-called "thematic" warrants…*

- *Secondly, we scrutinise the selected warrants and associated documentation in detail during reading days which precede the inspections.*
- *Thirdly, we identify those warrants, operations or areas of the process where we require further information or clarification and arrange to interview relevant operational, legal or technical staff, and where necessary we require and examine further documentation or systems in relation to those matters during the inspections."*

72. In addition, the Commissioner moved to a specific 5-phase inspection model for GCHQ, reflecting the type and scale of the interception it undertakes, involving a formal inspection for each of the 5 phases concerned, together with ad hoc visits in between (see 2015 Annual Report, §§6.79-6.84):

*"Phase 1: Warrantry process - ….an evaluation of the systems in place for the interception of communications to ensure they are sufficient; and examination of selected interception applications to assess whether they meet the requirements of necessity and proportionality; interviews with case officers, analysists and/or linguists from selected investigations or operations to assess whether the interception and the justification for acquiring all of the material were proportionate; examination of any urgent oral approvals to check the process was justified and used appropriately; a review of those cases where communications subject to legal professional privilege or otherwise confidential information (e.g. confidential journalistic or confidential medical) have been intercepted and retained, and any cases where a lawyer is the subject of an interception.*
*Phase 2: GCHQ Audits – this phase will cover scrutinising the results of the audits conducted by GCHQ on systems containing intercepted material and related communications data (as mentioned earlier in this section of the report). [The Commissioner] will also now participate in some of the system audits to provide independent verification.*
*Phase 3: Safeguards – On an annual basis [the Commissioner] will require an update on any changes to the retention, storage and deletion arrangements for systems containing intercepted material and related communications data and will scrutinise those changes to ensure compliance with section 15 of RIPA…*
*Phase 4: Sharing of intercepted material and related communications data with international partners – We commissioned an investigation in 2015 into the arrangements in place within GCHQ for the sharing of intercepted material and related communications data with foreign partners in order to review compliance with the section 15 safeguards…*
*Phase 5: Error investigations. We will require annual analysis of any trends or patterns in errors and a review of the measures put in place to prevent recurrence…"*

73. For completeness, the Commissioner's oversight of the acquisition of communications data under Chapter II Part I RIPA has been no less detailed: see e.g. Section 7 of the 2015 Annual Report, pp. 42-71, summarising the exercise of the Commissioner's powers in this respect.

74. The Commissioner has produced detailed written reports and recommendations after his inspections of the Intelligence Services, which are sent to the head of the relevant Intelligence Service and copied to the relevant Secretary of State and warrant granting department (2015 Annual Report at §6.44).

75. In addition to these regular inspections, the Commissioner had power to (and did) investigate specific issues. Thus, the Commissioner has undertaken "extensive investigations" into the media stories derived from material said to have been disclosed by Edward Snowden, insofar as they concern allegations of interception by UK agencies. The conclusions of those investigations are set out in the Commissioner's 2013 Annual Report, especially Section 6 (See Annex 11, **CB/35**).

76. S. 58 RIPA imposes important reporting duties on the Commissioner[48]. (It is an indication of the importance attached to this aspect of the Commissioner's functions that reports are made to the Prime Minister.) Reports must be made every 6 months, and laid before each House of Parliament. In this way, the Commissioner's oversight functions help to facilitate Parliamentary oversight of the activities of the Intelligence Services (including by the ISC). The Commissioner is also under a duty to report to the Prime Minister any contravention of RIPA which was not already the subject of a report by the IPT; and to report to the Prime Minister if it appears to him that arrangements for handling intercept material under s.15 or 16 RIPA are inadequate (see s.58 RIPA and §7.1 of the Code).

77. The Commissioner's oversight functions are supported by the record keeping obligations imposed as part of the s. 8(4) Regime. See §§6.27-6.28 of the Code. In practice, all the agencies that are empowered to conduct interception have arrangements in place with the Commissioner to report errors that arise in their interception operations[49]. The Commissioner addresses such errors in his six-monthly reports (see *e.g.* §§3.58-3.68 of the 2013 Annual Report).

78. In sum, as the Court rightly observed at §166 of its judgment in *Kennedy,* the Commissioner's role is of great importance as a safeguard (and it has been strengthened since *Kennedy* was decided):

> *"The Court considers that the Commissioner's role in ensuring that the provisions of RIPA and the Code are observed and applied correctly is of particular value and his biennial review of a random selection of specific case in which interception has been authorised provides an important control of the activities of the intercepting agencies and of the Secretary of State himself."*

*The Commissioner's views on the practical operation of the s. 8(4) Regime*

79. In §6.5.1 of his 2012 Annual Report (**CB/36**), the Commissioner stated that "*GCHQ staff conduct themselves with the highest levels of integrity and legal compliance*" [see Annex 37]. In §6.5.2 of that report, he observed that "*officers working for SIS conduct themselves in accordance with the highest levels of ethical and legal compliance*". As regards the Security Service, §6.5.4 of the 2012 Annual Report records: "*I was again impressed by the attitude and expertise of the staff I met who are involved in the interception of communications and I am satisfied that they act with the highest levels of integrity*." To similar effect, the Commissioner concluded as follows in his 2013 Annual Report:

[48] Parallel duties are now imposed upon the Investigatory Powers Commissioner by the Investigatory Powers Act 2016. His reports are annual: see s.234 Investigatory Powers Act 2016.
[49] Parallel arrangements have of course now been put in place with the Investigatory Powers Commissioner.

*"Our inspections and investigations lead me to conclude that the Secretaries of State and the agencies that undertake interception operations under RIPA 2000 Chapter I Part I do so lawfully, conscientiously, effectively and in the national interest. This is subject to the specific errors reported and the inspection recommendations. These require attention but do not materially detract from the judgment expressed in the first sentence."* See Annex 11, **CB/37**.

80. In his 2014 Annual Report (**CB/38**), the Commissioner indicated that he had undertaken a detailed investigation into GCHQ's[50] application of individual selection criteria from stored selected material initially derived from s.8(4) interception, reviewing the *"breadth and depth of the internal procedures for the selection of material to ensure that they were sufficiently strong in all respects"*. He concluded that, although there was no pre-authorisation or authentication process to select material, and consideration should be given to whether such a process was feasible or desirable, the selection procedure *"is carefully and conscientiously undertaken both in general and, so far as we were able to judge, by the individuals themselves"*, and *"random audit checks are conducted retrospectively of the justifications for selection, by or under the direction of GCHQ's Internal Compliance Team, and in addition, the IT Security Team conducts technical audits to identify and further investigate any possible unauthorised use",* which was *"a strong safeguard"*: see the 2014 Report, §§6.38-6.39.

81. The Commissioner also stated at §6.40 of the 2014 Report:

*"The related matters that my office investigated included the detail of a number of other security and administrative safeguards in place with GCHQ (which are not just relevant to interception work). These included the security policy framework (including staff vetting), the continuing instruction and training of all relevantly engaged staff in the legal and other requirements of the proper operation of RIPA 2000 with particular emphasis on Human Rights Act requirements, and the development and operation of computerised systems for checking and searching for potentially non-compliant use of GCHQ's systems and premises. I was impressed with the quality, clarity and extent of the training and instruction material and the fact that all staff are required to undertake and pass a periodic online test to demonstrate their continuing understanding of the legal and other requirements."*

## III THE QUESTIONS POSED BY THE COURT

### Question 1: Can the applicants claim to be victims, within the meaning of Article 34 of the Convention, of the alleged violations?

82. The answer to this question is "no", as concerns (i) the complaints by BBW and 10 HR relating to the Intelligence Sharing Regime; and (ii) BIJ's complaint concerning s.22 RIPA, which is brought on a fundamental misunderstanding of the facts and law.

### *The BBW and 10 HR complaints concerning the alleged sharing of material obtained under Prism/Upstream*

[50] The Commissioner focused upon GCHQ as "the interception agency that makes most use of section 8(4) warrants and selection criteria": see the 2014 Annual Report, §6.37.

83. The Applicants do not contend, and have put forward no evidential basis for contending, that their communications have in fact been intercepted under Prism/Upstream, and subsequently shared with the Intelligence Services. Rather, they assert only that their communications *"may be"* subject to foreign interception conveyed to UK authorities[51], or that they *"believe"* that to be the case[52]. In the circumstances, that mere assertion does not begin to establish that the Applicants are "directly affected" by the Intelligence Sharing Regime, such that they have victim status for the purposes of Article 34 ECHR. Their complaint is in truth an abstract complaint about the regime itself, which the Court should not entertain.

84. The Grand Chamber has recently considered the Court's own case law and clarified the conditions under which an applicant can claim to be a victim of secret surveillance measures violating Article 8 ECHR, without having to prove that secret surveillance measures have in fact been applied to him: see *Zakharov v Russia*. *Zakharov* notes, and resolves, a potential divergence in the Court's case law between those cases suggesting that general challenges to the relevant legislative regime would be permitted in such circumstances, and those suggesting that the relevant security agencies must be reasonably likely to have applied the measures in question to the applicant. See *Zakharov* at §§164-172. The Government assumes (in the Applicants' favour) that the principles in *Zakharov* may also apply to a claim of violation of Article 8 concerning the receipt of secret intelligence from a foreign state.

85. Two conditions must be satisfied before an applicant can claim to be the victim of a relevant violation without needing to show his communications have been interfered with – see *Zakharov* at §171:

> *"Accordingly, the Court accepts that an applicant can claim to be the victim of a violation occasioned by the mere existence of secret surveillance measures, or legislation permitting secret surveillance measures, if the following conditions are satisfied. Firstly, the Court will take into account the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted. Secondly, the Court will take into account the availability of remedies at the national level and will adjust the degree of scrutiny depending on the effectiveness of such remedies."* (Emphasis added)

86. As to the second condition (the availability of national remedies), where the domestic system affords no effective remedy to a person who suspects he has been the victim of secret surveillance, an exception to the rule that individuals may not challenge a law *in abstracto* is justified. However, if the national system provides for effective remedies, as in the present case, an individual may claim to be a victim of a violation occasioned by the mere existence of secret measures only if he is able to show that, due to his personal situation, he is potentially at risk of being subjected to such measures: *Zakharov* at §171.

[51] See BBW Application, §§10-17.

[52] See 10 HR Application, §8.

87. Here, neither of the two conditions in §171 of *Zakharov* is satisfied. *First,* the Applicants do not belong to the group of persons who may be said to be possibly affected by the Intelligence Sharing Regime. They have put forward no basis on which they are at realistic risk of having their communications intercepted under the Prism or Upstream programmes, and shared with the Intelligence Services. In particular:

(1) The Prism and Upstream programmes permit the interception and acquisition of communications to, from or about specific tasked selectors associated with non-US persons who are reasonably believed to be outside the US. I.e. they concern unanalysed intercepted communications (and associated communications data) relating to particular individuals outside the US, not broad data mining.
(2) As stated in the Disclosure, the Intelligence Services have only ever made a request for such unanalysed intercepted communications (and associated communications data) where a RIPA warrant is already in place for that material, but the material cannot be collected under the warrant[53]. Any request made in the absence of a warrant would be exceptional, and would be decided upon by the Secretary of State personally: see the Code at §12.3.
(3) The conditions for intercepting communications pursuant to a RIPA warrant are as set out in s.5(3) RIPA. They are the interests of national security; the prevention or detection of serious crime; or the safeguarding of the UK's economic well-being, in circumstances appearing relevant to the interests of national security. Those conditions substantially mirror the statutory functions of the Intelligence Services under the SSA and ISA.
(4) None of the Applicants suggest that their data could be collected and shared under any of the conditions in s.5(3) RIPA. In each case, they claim that their data may be shared with the UK because of their human rights activities, or campaigning activities concerning freedom of expression. Such activities would not give any grounds for the issue of a warrant for interception of the Applicants' communications under s.5(3) RIPA. Nor, by the same token, would they give grounds for intelligence sharing without a warrant in pursuance of the Intelligence Services' statutory functions. The Applicants do not contend otherwise.

88. *Secondly***,** the Applicants have available a remedy at national level, under which they can discover whether they have been the subject of unlawful intelligence sharing. That is a complaint to the IPT. The 10 HR Applicants complained to the IPT about whether they might have been subject to unlawful intelligence sharing. The IPT, having investigated the facts in detail, determined that they had not been. The BBW Applicants failed to complain to the IPT altogether.

89. The effectiveness of the IPT is well demonstrated by its careful and exhaustive consideration of the relevant legal regime and of the Applicants' own communications in the Liberty proceedings. In circumstances where the Applicants either have had recourse, or should have had recourse, to an effective domestic tribunal, which could have made findings of unlawfulness if warranted, it is unnecessary and inappropriate for the Court to entertain an abstract challenge to the Intelligence Sharing Regime as a whole.

[53] See the IPT's 5 December Judgment, [48(2)].

***The BIJ complaint concerning s.22 RIPA***

90. The factual premises for BIJ's Application concern the interception of their communications by GCHQ's alleged Tempora operation. In other words, those factual premises are the same ones about the s.8(4) Regime at issue in all 3 Applications. See §§24-28 of the BIJ Application[54].

91. If such interception were to take place, it would take place pursuant to the authority of an interception warrant under Chapter 1 of Part 1 RIPA (see **CB/22**).

92. Section 22 RIPA is a provision of an entirely different type, and falls within Chapter 2 (not Chapter 1) of Part 1 RIPA. In brief summary, it gives power to certain designated persons to issue a notice to a postal or telecommunications operator, requiring them to provide specified communications data. A notice may be issued where the designated person believes it necessary on one or more of the grounds listed in s.22(2). Those grounds include the interests of national security and the prevention or detection of crime. By definition, the obtaining of communications data in this way does not involve the interception of communications in the course of their transmission. Pursuant to s.21(1) RIPA, Chapter 2 of Part 1 RIPA applies to:

> *"(a) any conduct in relation to a postal service or telecommunications system for obtaining communications data, other than conduct consisting in the interception of communications in the course of their transmission by means of such a service or system; and*
> *(b) the disclosure to any person of communications data."*(Emphasis added)

"*Interception in the course of transmission*", it may be noted, is a broad definition. It includes interception of data while it is stored on a telecommunications system, as well as while it is passing over the system[55].

93. Thus the BIJ Application is brought on a fundamental legal misunderstanding about the nature and scope of activity authorised by s.22 RIPA.

94. Specifically, the BIJ Applicants wrongly assume[56] that the s.8(4) Regime is concerned only with the interception of communications, and the s.22 Regime with the interception of communications data. The true position, of course, is that the s.8(4) Regime is concerned both

[54] The Applicants' recent letter of 18 July 2017 attempts to circumvent this misunderstanding by contending that their Application concerns "*the solicitation and receipt of communications data by the intelligence services, intercepted by a telecommunications operator and then disseminated to the intelligence services".* That contention fails to address the factual premises for their Application. It thus ignores the fact that they have put forward no factual basis whatsoever to suggest that their communications data has been "disseminated" to the Intelligence Services.

[55] See s.2(7) RIPA: *" For the purposes of this section the times while a communication is being transmitted by means of a telecommunication system shall be taken to include any time when the system by means of which the communications is being, or has been, transmitted is used for storing it in a manner that enables the intended recipient to collect it or otherwise to have access to it."*

[56] See in particular §§91-94 of the BIJ Obs in Reply, and §§157-158 of the Application.

with the interception of communications *and* related communications data[57]; and the s.22 Regime is not concerned with any interception at all, whether of communications or communications data.

95. It follows that the BIJ Applicants have put forward no factual basis whatsoever for concluding that their communications data have been the subject of any notice issued under s.22 RIPA. Neither Applicant contends that data relating to any of their communications have been the subject of a notice issued, or authorisation granted, under s.22 RIPA. They do not contend that they have been affected, either directly or indirectly, by a notice issued under s.22 RIPA. The facts they plead entirely concern the wholly different circumstances of interception under a s.8(4) warrant.

96. Furthermore, neither of the two specific conditions identified by the Court at §171 of *Zakharov* is satisfied in respect of the s.22 Regime.

97. As to the first condition, the Applicants do not belong to a group 'targeted' by the contested legislation. The s.22 Regime is not targeted at journalists, and an authorisation could potentially be granted in respect of the communications data of any individual. Specific provision is made in the Acquisition and Disclosure Code concerning journalistic sources, and to that extent the Applicants are, in effect, granted special exemption from the ordinary application of the s.22 Regime. Nor can it be said that the legislation '*directly affects all users of communication services'* in the manner addressed by the Court in *Zakharov*. A s.22 authorisation applies only to those specific communications data and persons in respect of which it is granted. The authorisation can only be granted on one of a number of specific grounds, and is subject to an overriding requirement of proportionality[58].

98. As to the second condition, the Applicants have available a remedy at national level, which is effective, and which they have failed to use. The IPT has power to investigate any allegation of unlawfulness in relation to the obtaining of communications data under s.22 RIPA, including any allegations that (i) the obtaining of communications data is unlawful because the legal framework in Chapter 2 Part 1 of RIPA is not "in accordance with the law" for the purposes of Article 8/10; and (ii) the obtaining of communications data is disproportionate (those being the contentions the BIJ Applicants make[59]). Indeed, the effectiveness of the IPT in these circumstances is illustrated by its recent decision in *News Group Newspapers Limited v Metropolitan Police Commissioner*

[57] The conduct authorised by interception warrants issued under s.5(1) RIPA includes, pursuant to s.5(6) RIPA, *"conduct for obtaining related communications data". "Related communications data"* is defined by s.20 RIPA to be so much of any communications data as (a) is obtained by, or in connection with, the interception; and (b) relates to the communications.

[58] The degree of specificity that will be required in an application in order to demonstrate that the test of necessity is met is explained at §§2.37-2.38 of the Acquisition and Disclosure Code. As a minimum, the application must specify: the event under investigation; the person concerned and how they are linked to the event; and the communications data that is being sought (such as a telephone number or IP address) and how the data is related to the person and the event.

[59] See §§158 and 162 of the Application.

UKIPT/14/176/H[60], where it quashed an authorisation under s.22 RIPA obtained by the Metropolitan Police. If the Applicants wished to assert that their factual circumstances gave rise to a particular risk that GCHQ might have obtained their communications data pursuant to a notice under s.22 RIPA, they could have made that allegation to the IPT; and the IPT would have investigated it.

99. In sum, this is an *in abstracto* challenge, brought on a fundamental misunderstanding of the law and/or the facts, to which the 'general approach' identified in *Zakharov* should apply.

**Question 2: If the Applicants did not raise their Convention complaints before the IPT, have they done all that is required of them to exhaust domestic remedies?**

100. The answer to this question is "no" as concerns the BBW and BIJ Applicants, who did not raise their Convention complaints before the IPT, for the following reasons:

(1) The IPT is a bespoke domestic tribunal set up for the very purpose of investigating, considering and ruling on precisely the issues raised by the Court's questions. That it is accessible is obvious from the Liberty proceedings and undisputed.
(2) It is a tribunal which, as the Court held in *Kennedy v UK*, is Article 6 compliant. Its consideration of and rulings on cases falling within its jurisdiction (as these claims undoubtedly would have done) therefore comply with the procedural requirements laid down by the Convention.
(3) It is capable of providing redress in respect of the complaints made – as is demonstrated by the manner in which it has dealt with similar cases (including the Liberty case).
(4) There are particular advantages in having the IPT consider complaints prior to this Court considering compliance with the Convention. Not merely is that sequence in line with the constitutional scheme of the Convention (recently emphasised in eg. the Brighton Declaration and Protocol 15[61]). It also enables the Court to have the benefit of the IPT's detailed assessment of the operation of the relevant domestic legal regime, on the basis of a close knowledge and understanding of that system. The alternative is a potential flood of applications direct to the Court, without either the filter or the benefits of consideration by the bespoke domestic tribunal.

***Subsidiarity and the exhaustion of domestic remedies***

101. There is an increasing emphasis in the case law of the Court on the importance of

[60] See Annex 45

[61] Ratified by the UK on 10 April 2015, but yet to enter into force pending ratification by all signatories to the ECHR. (see Annexes 38 and 39).

subsidiarity, both in terms of the margin of appreciation given to member states[62], and in terms of the importance of exhausting domestic remedies. This is a reflection of the status of these concepts in the Convention machinery[63] - as set out in the Brighton Declaration[64] and Protocol 15[65] in June 2013, adding a direct reference to the concepts of subsidiarity and the margin of appreciation in the preamble to the Convention[66].

102. The Grand Chamber recently reiterated in *Vuckovic & Others v Serbia* app. Nos. 17153/11 et al, 25 March 2014, that a fundamental feature of the machinery of protection established by the Convention is its subsidiarity to the national systems safeguarding human rights; that the Court should not take on the role of Contracting States, and is not a court of first instance; that the rule of exhaustion of domestic remedies is therefore an *"indispensable part of the functioning of this system of protection";* and that States are *"dispensed from answering before an international body for their acts before they have had an opportunity to put matters right through their own legal systems".* See §§69-71.

103. Similarly in *Roberts v United Kingdom*, app. 59703/13, 28 January 2016, the Court emphasised the "indispensable" role of exhaustion of domestic remedies. At §37 it stated:

> "*It is primordial that the machinery of protection established by the Convention is subsidiary to the national systems safeguarding human rights. This Court is concerned with the supervision of the implementation by Contracting States of their obligations under the Convention. It cannot, and must not, take on the role of Contracting States whose responsibility it is to ensure that the fundamental rights and freedoms enshrined therein are respected and protected on a domestic level. The rule of exhaustion of domestic remedies is therefore an indispensable part of the functioning of this system of protection. States are dispensed from answering before an international body for their acts before they have had an opportunity to put matters right through their own legal system and those who wish to invoke the supervisory jurisdiction of the Court as concerns complaints against a State are thus obliged to use first the remedies provided by the national legal system..."*

---

[62] See, for example, *Animal Defenders International v United Kingdom* app. 48876/08, 22 April 2013 at §§115-117, *SAS v France* app. 43835/11, 1 July 2014 at §129, §154, *Lambert v France* app. 460/43/14, 5 June 2015 at §§144-148, §168, and *Parillo v Italy* app. 464/70, 27 August 2015 at §169, §175, §§183-188.

[63] As reflected in the Interlaken (2010) and Izmir (2011) discussions and declarations and the Brighton Declaration of April 2012.

[64] Which states, *inter alia*, at §15:*"The Conference therefore: ... g) Invites the Court to develop its case law on the exhaustion of domestic remedies so as to require an applicant, where a domestic remedy was available to them, to have argued before the national courts or tribunals the alleged violation of the Convention rights or an equivalent provision of domestic law, thereby allowing the national courts an opportunity to apply the Convention in light of the case law of the Court."*

[65] Which was ratified by the UK on 10 April 2015 (although it will not enter into force until ratified by all ECHR signatories).

[66] At the end of the preamble to the Convention, a new recital was added, which states: "*Affirming that the High Contracting Parties, in accordance with the principle of subsidiarity, have the primary responsibility to secure the rights and freedoms defined in this Convention and the Protocols thereto, and that in doing so they enjoy a margin of appreciation, subject to the supervisory jurisdiction of the European Court of Human Rights established by this Convention*,"

104. Consequently, it is appropriate that the national courts should initially have the opportunity to determine questions regarding the compatibility of domestic law with the Convention[67]. Not only are they better placed than the Court to establish facts that may be relevant to victim status and any proportionality assessment, but the Court is likely to benefit from the national courts' views on the compatibility of domestic law: particularly where (as here) the law is complex.

105. As emphasised in *Vuckovic* it is also important that member states are given the opportunity to *'put matters right'* through their own legal system before the matter comes before the ECtHR[68]. That is based on the assumption, reflected in Article 13, that the domestic legal order will provide an effective remedy for violations of Convention rights. This is particularly important in common-law systems. As the ECtHR stated in *Upton v the United Kingdom* (Application No 29800/04), at p. 8, in a common law system, where the courts extend and develop the principles through case law, *"it is generally incumbent on an aggrieved individual to allow the domestic courts the opportunity to develop existing rights by way of interpretation"*.

106. Further, the Court recognised in *Kennedy v United Kingdom* that the extensive powers of the IPT and their access to confidential information has a "*special significance*" in the context of secret surveillance measures (see §110).

107. It is also important that the current context involves an assessment of issues of necessity and proportionality, which is particularly difficult to undertake without a proper determination at the national level of facts material to the balance between the rights of the individual and the interests of the community as a whole.

***The effectiveness and benefits of the IPT***

108. The IPT provides one of the most far-reaching systems of judicial oversight over intelligence matters in the world. As is apparent from the summary of the IPT's powers and practice at §§58-66 above, the IPT's jurisdiction and remedial powers are very board. It is this tribunal which the BBW and BIJ Applicants assert can effectively be bypassed.

109. The substantive complaints under Articles 8 and 10 in these cases focus on an alleged lack of publicly available safeguards and upon proportionality. The IPT has the jurisdiction and the requisite powers to deal with all aspects of those complaints:

(1) The IPT can (and did in the Liberty Proceedings) make clear the extent to which the relevant domestic regime is compatible with Article 8 and/or Article 10 ECHR and, if the regime is not compatible, it can identify the respects in which the regime is deficient.

[67] See also *A, B and C v Ireland* app. 25579/05, 16 December 2010 (Grand Chamber) at §142 and *Burden v United Kingdom* app. 13378/05, 29 April 2008, at §42.

[68] See also *Akdivar v Turkey* §65 and *Cardot v France* app. at §§34-36 where the ECtHR stated that "*any procedural means which might prevent a breach of the Convention should have been used*".

(2) Thus, if there is a lack of foreseeability in the regime, despite adequate substantive safeguards in fact being in place, the IPT can identify with precision the respects in which the safeguards which are applied are not (and should be) public. That means those particular aspects can be remedied as necessary by the Government, for example with further disclosure and/or changes to the applicable Code. Indeed, the very process of scrutiny in the IPT provides an important opportunity to address any lack of foreseeability in the regime, as occurred with the further Disclosure in the Liberty proceedings.

(3) Further, in circumstances where proportionality is in issue (as here), the IPT, with its ability to consider relevant intelligence material in closed proceedings, is able to provide an effective remedy. It has the power to quash s.8(4) warrants and order the destruction of data. It is able to consider the factual circumstances of individual complainants and to make individual determinations in favour, as occurred in the Liberty and the *Belhaj*[69] proceedings, together with such reasons as are appropriate. In that regard it is to be noted that reasons have been given in these cases (see also the ECtHR's observations in *Kennedy* at §189[70]).

110. In addition, there are very considerable benefits to having the IPT consider and determine the complaints prior to this Court considering them.

111. **First,** it produces open judgments to the extent that it can do so consistently with the public interest, including the needs of national security. Whilst the open judgments may (for good reasons of national security and the protection of the public interest) necessarily be based on assumed facts, the IPT's own detailed consideration of the applicable legal regime is important: particularly where, as here, that framework is complex.

112. **Secondly,** the IPT will investigate and consider in closed session such sensitive material as is relevant to the complaints. It then produces its decisions having regard to that closed material. That closed material may relate e.g. to the internal arrangements and safeguards which are operated by the Intelligence Services and which, for reasons of national security, cannot be disclosed. It may also relate to the factual position *vis à vis* individual complainants and/or to the intelligence picture insofar as that is relevant to the proportionality of particular intelligence regimes/techniques.

113. That access to closed material, coupled with the extensive disclosure duties which arise in IPT proceedings, puts the IPT in a special position. It means that the IPT's open determinations are determined with the benefit of knowledge of the full factual position in closed. That enables the IPT, for example:

(1) to assess whether the Intelligence Agencies' internal arrangements/safeguards are, in fact, in place, in accordance with the publicly available regime;

(2) to evaluate the adequacy and effectiveness of those internal arrangements/safeguards;

---

[69] *Belhaj and others v Security Service and others* UKIPT/13/132-9H, Annex 43

[70] Where the Court stated: "*The Court further notes in this regard that, in the event that a complaint is successful, the complainant is entitled to have information regarding the findings of fact in his case*".

(3) to make an assessment as to whether more needs to be said about those arrangements/safeguards in open;
(4) To make a proper assessment of proportionality, by taking into account all factors relevant to the respective balance of interests, including those which cannot be disclosed for reasons of national security.

***Developments since Kennedy***

114. In the light of the matters set out above, and the Court's increasing emphasis on subsidiarity, it is submitted that the position has moved on since *Kennedy* - see §§108-112 and the Court's conclusions on non-admissibility in that case. At the time of *Kennedy* the Court was of the view that it was "*less clear*" whether the IPT's extensive powers to access confidential information were relevant where the complaint was one of a general nature, rather than a specific complaint of interception in an individual case (see §110). But, for the reasons set out above, the benefits of the IPT's specialist regime, even in the case of general challenges, are now self-evident. It is hard to see, for example, how the elucidation of the general regimes which occurred in the Liberty proceedings is not of considerable assistance to this Court, particularly where the relevant regimes consist of a complex interlocking framework of safeguards, including internal arrangements operated by the Intelligence Services.

115. It is no answer to these points to seek to rely upon the fact that the IPT has no jurisdiction to make a declaration of incompatibility under s.4 of the Human Rights Act 1998.

116. **First**, as is evident from the description of the IPT's powers above, it has a range of remedies at its disposal that supplement its declaratory jurisdiction, which provide redress in an individual case. It can award compensation, order the destruction of data, quash a warrant, or do anything else necessary to provide an individual with a remedy for mistreatment of their data. So, to the extent that a complaint is based on an assertion of unlawfulness affecting the individual complainant, the IPT's jurisdiction needs to be invoked and the remedies it is capable of providing need to be exhausted. These complaints are all individual complaints – they challenge the general lawfulness of the relevant regimes but each also challenges individual lawfulness. Nothing in s.4 HRA touches this capacity to afford individual redress in appropriate cases, or in some way operates to excuse applicants to the Court from any need to complain first to the IPT.

117. **Secondly**, and in any event, even in relation to the IPT's more general declaratory jurisdiction, there is no remedial deficit in Convention terms. The IPT can and does rule on the general lawfulness of the regimes about which complaints are made. If it concludes that a regime is contrary to the Convention, it will so state. The reaction of the Government to such findings has been consistent. It has ensured that any defects are rectified and dealt with. That is demonstrated clearly by for example the Liberty and *Belhaj*[71] proceedings. So the proper conclusion *on the facts* is that a finding of incompatibility by the IPT would indeed be the effective trigger for the necessary changes to ensure Convention compatibility.

[71] See Annex 43

118. The Court is entitled to and should focus on the *practical* effectiveness of a particular remedy. If the Government has in practice reacted so as to remedy any concerns found, that is an important matter in the Court's assessment. As the Court held in *Leander v. Sweden*, 26 March 1987, Series A no.116 at §82, a consistent national practice and a tradition of respecting pronouncements which are not formally binding will be sufficient to satisfy the requirements of Article 13:

> *"The main weakness in the control afforded by the Ombudsman and the Chancellor of Justice is that both officials, apart from their competence to institute criminal and disciplinary proceedings, lack the power to render a legally binding decision. On this point, the Court, however, recalls the necessarily limited effectiveness that can be required of any remedy available to the individual concerned in a system of secret security checks. The opinions of the Parliamentary Ombudsman and the Chancellor of Justice command by tradition great respect in Swedish society and in practice are usually followed. It is also material—although this does not constitute a remedy that the individual can exercise of his own accord—that a special feature of the Swedish personnel control system is the substantial parliamentary supervision to which it is subject, in particular through the parliamentarians on the National Police Board who consider each case where release of information is requested."*

119. Accordingly the Government submits that these complaints should be rejected in accordance with Article 35(4).

**Question 3(a): are the acts of the United Kingdom's Intelligence Services in relation to the soliciting, receipt, search, analysis, dissemination, storage and destruction of interception data obtained by the intelligence services of other States in accordance with the law/necessary under Articles 8 and 10?**

***The Intelligence Sharing Regime is "in accordance with the law"***

120. The expression "in accordance with the law" in Article 8 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*, §84).

121. The test for whether an interference is "prescribed by law" for the purposes of Article 10 ECHR does not differ at all in this context, and the Court commonly addresses Articles 8 and 10 together in circumstances analogous to these: see e.g. *Telegraaf Media v The Netherlands* App. no. 39315/06, 22 November 2012, at §90.

122. The interferences at issue plainly have *a basis in domestic law*. The statutory provisions in the Intelligence Sharing Regime[72] provide domestic law powers for the obtaining and subsequent use of communications and communications data in issue (assuming that this is necessary for one or more of the functions of the Intelligence Service in question, and proportionate for the purposes of s.6(1) HRA). That satisfies the requirement that the regime have a basis in domestic law. The Applicants' arguments to the contrary[73] are on a proper analysis complaints about the foreseeability of domestic law, rather than the regime's legal basis.

123. The law in question is clearly "*accessible*". It is set down in statute, and supplemented by chapter 12 of the Code. (Indeed, even prior to the issue of chapter 12 of the Code, it was "accessible" as a result of the Disclosure[74]). For these purposes, case law may form part of a corpus of accessible law: see e.g. *Huvig v France* 24 April 1990, Series A no. 176-B at §28, *Uzun v Germany* app. 35623/05, ECHR 2010, at §33.)

124. As to *"foreseeability"* in this context, the essential test, as recognised in §68 of *Malone v UK* (app. 8691/79), 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*". The Grand Chamber has confirmed in *Zakharov* that this test remains the guiding principle when determining the foreseeability of intelligence-gathering powers (see §230). Further, this essential test must always be read subject to the important and well-established principle that the foreseeability requirement cannot mean that an individual should be enabled to foresee when the authorities are likely to resort to secret measures so that he can adapt his conduct accordingly: *Malone* at §67; *Leander v. Sweden*, 26 March 1987, Series A no.116, at §51; and *Weber* at §93. The Intelligence Sharing Regime satisfies this test.

125. **First**, the regime is sufficiently clear as regards the circumstances in which the Intelligence Services can in principle **obtain** information from the US authorities.

126. The purposes for which such information can be obtained are explicitly set out in ss.1-2 SSA, and ss.1-2 and 3-4 ISA (**CB/24-25**), which set out the functions of the Intelligence Services. They are the interests of national security, in the context of the various Intelligence Services' particular functions; the interests of the economic wellbeing of the United Kingdom; and the prevention and detection of serious crime. 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

[72] I.e. the SSA and the ISA, as read with the CTA; the HRA; the DPA; and the OSA. In particular, the statutory powers and functions in the SSA and ISA, exercisable for the purposes set out in those Acts and in accordance with s.6 HRA, and read with s.19(2) CTA, provide the requisite domestic law powers for the Intelligence Services' obtaining and subsequent use of communications and communications data from foreign partners. See §§2.2-2.9 of the BBW Observations.

[73] See e.g. §121 of the BBW Application

[74] Further, the Disclosure was embodied in a draft of the Code, published in February 2015, with which the Government undertook to comply. See Annex 44.

communications systems[75] - obtain communications and communications data from a foreign intelligence agency if that is *"in the interests of national security"*, with particular reference to the Government's defence and foreign policies (s.3(2)(a) ISA), or *"in the interests of the economic well-being of the United Kingdom"* (s.3(2)(b) ISA), or "*in support of the prevention or detection of serious crime*" (s. 3(2)(c) of ISA); provided always that it is also necessary and proportionate to obtain information for that purpose under s. 6(1) of the HRA (**CB/26**)[76].

127. Contrary to the Applicants' contentions, those purposes are not too broad to be "in accordance with law". In fact, they are no wider in substance than the statutory purposes for which an interception warrant could be issued under s.5 RIPA (prior to its amendment by DRIPA[77]). Indeed, in certain respects, they are more tightly defined than the conditions for obtaining a warrant under s.5 RIPA (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[78]).

128. The statutory purposes for issue of a warrant under s.5 RIPA (in its unamended form) were considered by the Court in *Kennedy* and were found sufficiently detailed to satisfy the requirement of foreseeability, even in the context of interception of communications by the defendant state itself. See *Kennedy* at §159.

129. The Court has more recently found those very same purposes sufficiently detailed to satisfy the "foreseeability" test in the context of covert surveillance pursuant to Part II RIPA: see *RE v United Kingdom* app. 62498/11, 27 October 2015, at §133 (citing *Kennedy* with approval). (By contrast, the cases upon which the Applicants rely– *Khan v United Kingdom* (app. 35304/97), ECHR 2000-V and *Halford v United Kingdom,* 25 June 1997, Reports of Judgments and Decisions 1997-III – are both ones concerning police surveillance, where there was at the relevant time no statutory framework regulating the conduct in question.)

---

[75] Such systems fall within the scope of s. 3(1)(a) of ISA by virtue of being "equipment" producing "electromagnetic, acoustic and other emissions".

[76] The BBW Applicants are wrong to assert (Application, §121) that the Intelligence Services may obtain information from foreign agencies "*for the purposes of any criminal proceedings*". The Intelligence Services are empowered to disclose information for the purposes of criminal proceedings (subject to other statutory safeguards upon such disclosure, such as the prohibition in s.17 RIPA on adducing intercept evidence in legal proceedings). However, such information can only be acquired in the first place if it is necessary and proportionate to do so for the statutory functions of the Services, set out above (which do not include the purposes of "any criminal proceedings"): see s.2(2)(a) SSA, and ss.2(2)(a) and 4(2)(a) ISA.

[77] See §3.66 of the Government's BBW Observations.

[78] 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.

130. Moreover, the circumstances in which the Intelligence Services may obtain information under the Intelligence Sharing Regime are further defined and circumscribed by the Code and Disclosure (which reflect what has always been the practice of the Intelligence Services). In particular, the Code provides the following public safeguards on obtaining information:

(1) Save in exceptional circumstances, the Intelligence Services will only make a request for unanalysed intercepted communications and associated communications data, otherwise than in accordance with an international mutual legal assistance agreement, if a RIPA warrant is already in place covering the target's communications; the assistance of the foreign intelligence agency is necessary to obtain the communications because they cannot be obtained under that RIPA warrant; and it is necessary and proportionate for the Intelligence Services to obtain those communications. It should be noted that the circumstances are sufficiently exceptional that they have not yet ever occurred[79].

(2) If the Intelligence Services were to make a request for such material in the absence of a RIPA warrant, they would only do so if the request did not amount to a deliberate circumvention of RIPA or otherwise frustrate the objectives of RIPA. So, for example, the Intelligence Services could not make a request for material equally available by interception pursuant to a RIPA warrant. However, they could make a request for material which it was not technically feasible to obtain under Part I RIPA, and which it was necessary and proportionate for them to obtain pursuant to s.6 HRA.

(3) Further, if the Intelligence Services were to make a request for such material in the absence of a RIPA warrant, that request would be decided upon by the Secretary of State personally; and if the request was for "untargeted" material, any communications obtained would not be examined according to any factors mentioned in s.16(2)(a) and (b) RIPA, unless the Secretary of State personally considered and approved the examination of those communications by reference to such factors. In short, the same safeguards would be applied by analogy, as if the material had been obtained pursuant to a RIPA warrant.

131. **Secondly**, the Intelligence Sharing Regime is similarly sufficiently clear as regards the subsequent handling, use and possible onward disclosure of communications and communications data obtained by the Intelligence Services.

132. Under statute, handling and use is addressed by (i) s. 19(2) of the CTA (**CB/28**)[80], 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 (**CB/23**) as regards security measures whilst the information is being stored.[81]

[79] See §48(2) of the IPT's 5 December judgment, Annex 15, **CB/14**

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

[81] As to the fifth and seventh data protection principles, it is no answer for the Applicants to point to the "explicit exemption from the data processing principles in the context of processing data in the interests of national security"

133. Moreover, additional safeguards as to the handling, use and onward disclosure of material obtained under the Intelligence Sharing Regime are provided by the Code. Specifically, chapter 12 of the Code provides that where the Intelligence Services receive intercepted communications content or data from a foreign state, irrespective whether it is solicited or unsolicited, analysed or unanalysed, and whether or not the communications data is associated with the content of communications, the communications content and data are subject to exactly the same internal rules and safeguards as the same categories of content or data, when the material is obtained directly by the Intelligence Services as a result of interception under RIPA. That has important consequences:

(1) It means that the safeguards set out in s.15 RIPA, as expanded upon in Chapter 7 of the Code, apply to intercept material obtained under the Intelligence Sharing Regime. So for example, just as under RIPA:
   i. The number of persons to whom the material is disclosed or otherwise made available, the extent to which it is made available, the extent to which it is copied, and the number of copies that are made, must be limited to the minimum necessary for the purposes authorised in s.15(4) RIPA.
   ii. The material (and any copy) must be destroyed as soon as there are no longer any grounds for retaining it as necessary for any of the authorised purposes in s.15(4) RIPA.
   iii. The arrangements for ensuring that (i) and (ii) above are satisfied must include such arrangements as the Secretary of State considers necessary to ensure the security of retained material: see s.15(5) RIPA.
   iv. The disclosure of intercepted material to authorities outside the UK is subject to the safeguards set out in §7.5 of the Code.

(2) It means that the internal rules and safeguards applicable to material obtained under the Intelligence Sharing Regime are *de facto* subject to oversight by the Commissioner, who offers an *"important safeguard against abuse of power"*: see s.57(2)(d) RIPA and *Liberty v UK* app. 58243/00, 1 July 2008 at §67.

134. **Thirdly**, when considering whether the Intelligence Sharing Regime is "*foreseeable*", the Court should take into account the available oversight mechanisms – namely, the ISC, the IPT, and (as set out above, with respect to oversight of the relevant internal "arrangements" themselves) the Commissioner. Those oversight mechanisms are important and effective, for all the reasons already set out. The relevance of oversight mechanisms in the assessment of foreseeability, and in particular the existence of adequate safeguards against abuse, is very well established in the Court's case law, including in this context (see e.g. *Kennedy* at §§155-170, *Zakharov* at §§271-280).

---

(BBW Application, §121.7). As explained in the summary in the Government's Observations of "domestic law and practice", the relevant certificates (which are publicly available) do not exempt the Intelligence Services from compliance with the fifth and seventh data protection principles.

135. The Court should also take into account in the foreseeability test, just as it did in *Kennedy* at §168, of the fact that the investigations by the oversight bodies have not revealed any deliberate abuse by the Intelligence Services of their powers. Neither the ISC nor Commissioner has found that the Intelligence Services have circumvented or attempted to circumvent UK law by receiving material under the Intelligence Sharing Regime, despite the fact that both of them have specifically investigated this allegation: see:

(1) the ISC's finding in its Statement of 17 July 2013 that the UK "*has not circumvented or attempted to circumvent UK Law*" by receiving material from the US[82];
(2) The Commissioner's rejection of 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*" (see his 2013 Annual Report at §§6.8.1-6.8.6[83]).

136. **Finally,** for the purposes of the foreseeability test, the Court should take into account too that the IPT has examined the Intelligence Services' internal safeguards in the context of the Intelligence Sharing Regime in detail, and has found that adequate internal safeguards exist[84], and that the Regime as a whole (with the benefit of the Disclosure, now mirrored in the Code) is in accordance with the law. The fact that the applicable internal safeguards have now been examined not just by the Commissioner, but also by the domestic courts, and have been found to offer sufficient protection for the purposes of rights under the ECHR, is an important indicator that the regime as a whole provides adequate safeguards against abuse.

*The Applicants' further contentions on "the Prism issue"*

137. The Applicants' first assertion is that, even if the Intelligence Sharing Regime is now "in accordance with the law" as a result of the Disclosure/Code, it was not in accordance with the law at the time of their applications, and the Court should so declare[85]. That argument is bad. The Court does not ignore developments since the lodging of an application in its assessment of the merits of a case; indeed, the BBW Applicants' Update Submissions themselves are lodged on the premise that the Court should take further developments into account. The question whether an applicant is a victim of a violation of the Convention is relevant at all stages of the proceedings under the Convention: see e.g. *X v Austria*, app. 5575/72, 8 July 75, D.R.1 p. 45, *HE v Austria* (app. 10668/83), 13 May 1987, *Burdov v Russia* app. 59498/00 at §30. The Applicants' challenge is to the Intelligence Sharing Regime itself, not to particular past acts carried out under that

[82] See Annex 21, **CB/43**. The investigation that preceded the ISC's Statement was thorough. See §5 of the Statement.

[83] See Annex 11, **CB/35**

[84] See [55] of the IPT's 5 December Judgment: *"Having considered the arrangements below the waterline, as described in the judgment, we are satisfied that there are adequate arrangements in place for the purpose of ensuring compliance with the statutory framework and with Articles 8 and 10 of the Convention, so far as the receipt of intercept from Prism and/or Upstream is concerned."*

[85] See e.g. BBW Update Submissions §§84-85, 10 HR Obs in Reply §249.

regime. If the Intelligence Sharing Regime is now in accordance with the law, the Applicants can no longer claim to be victims of it.

138. The Applicants then put forward three reasons why they now say the Intelligence Sharing Regime remains not "in accordance with the law", even following the Disclosure, as mirrored in the Code. First, they say that the six "minimum safeguards" to which the Court referred at §95 of *Weber*[86] ("the *Weber* criteria") should apply where intercept material is obtained from a foreign State, and be set out in statute[87]. Secondly, they say that the Disclosure is insufficient as a safeguard, is "*obscurely drafted and vague*" and does not amount to "law"[88]. Thirdly, they say that there should be "prior independent authorisation" or a requirement for "reasonable suspicion" (contentions that they also make with regard to the s.8(4) Regime)[89]. None of those arguments is sustainable.

139. As to the first argument, the IPT was entirely correct to conclude at §41 of the 5 December Judgment that in this context the *Weber* criteria (or *"nearly Weber"* criteria) do not apply. And even if such criteria were to apply, it would not be necessary or appropriate to set them out in statute. *Weber* concerns interception **by the respondent State**. The Applicants do not cite any Art. 8 (or Art 10) 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. 8/10 to cases of this latter type has never been considered by this Court.

140. 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 Services have merely obtained information from a foreign State, but there are also very good reasons why that should not be so.

141. **First**, this Court has expressly recognised that the "rather strict standards" developed in the recent Strasbourg intercept cases do not necessarily apply in other intelligence-gathering contexts: see e.g. *Uzun v. Germany* at §66. Further, this Court has never suggested that this form of wide-ranging and detailed scheme is necessary for intelligence sharing with foreign intelligence agencies (and see §96 of *S and Marper v. UK* (GC) nos. 30562/04 and 30566/04, ECHR 2008: domestic legislation "*cannot in any case provide for every eventuality*").

---

[86] "*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).

[87] See e.g. BBW Update Submissions §85, 10 HR Obs in Reply §§235-245.

[88] See 10 HR Obs in Reply §248.

[89] See 10 HR Obs in Reply §247.

142. **Secondly,** this Court has made clear subsequent to *Weber* in *Liberty, Kennedy* and *Zakharov* that even in the context of interception by the respondent State it is not necessary for every provision/rule to 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* as regards the Code. That position has now been confirmed by the Grand Chamber in *Zakharov,* which refers to the need for the *Weber* criteria to be set out *"in law",* rather than in statute: see *Zakharov* at §231.

143. **Thirdly**, there is no good reason to single out intercepted 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, or covert audio / visual surveillance. In many contexts, the Intelligence Services may not even know whether communications provided to them by a foreign intelligence agency have been obtained as a result of interception[90]. Moreover, 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 other types of intelligence (Farr §§27-30, Annex 3, **CB/9**). Thus, it would be nonsensical if Member States were required to comply with the *Weber* criteria for receipt of intercept material from foreign States; but were not required to do so for any other type of intelligence that foreign States might share with them.

144. **Fourthly**, it would plainly not be feasible (or, from a national security perspective, safe) for a domestic legal regime to (i) set out in publicly accessible form (let alone set out in statute) <u>all</u> the various types of information that might be obtained, whether pursuant to a request or not, 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 e.g. Farr §§56-61.

145. **Finally,** if (contrary to the above) the *Weber* criteria were to apply in this context, the Intelligence Sharing Regime satisfies each of the six criteria through a combination of the statutory provisions governing the receipt of intelligence, and the Code, for the reasons already set out at §§125-133 above. It describes:

(1) the nature of the offences which may lead to intelligence being obtained and the persons whose communications may be obtained. Those matters are implicit within the statutory description of the purposes of which intelligence may be obtained: see §§125-129 above;

(2) the limits on the duration of such obtaining (since a RIPA warrant will be in place, save in exceptional circumstances, and such a warrant has clear limits on duration);

[90] The Applicants assert that the Disclosure and Code show that the Government has *"no difficulty distinguishing [intercept] from other material the UK Intelligence Services receive":* see §240 of the 10 HR Obs in Reply. That assertion ignores the fact that the Disclosure/Code apply to intercepted material that is either requested, or which identifies itself as the product of interception. For obvious reasons, the Intelligence Services may well receive other intercept material which does not identify itself as the product of interception.

(3) the process for examining, using and storing data (since parallel safeguards to those under RIPA apply); and
(4) the circumstances in which the material may be erased/destroyed (since the material is treated in the same way as comparable material obtained under RIPA).

146. As to the second argument, the Code itself mirrors the Disclosure. The Code is "law" for the purposes of the "in accordance with the law" test: see e.g. *Kennedy*. (Moreover, the Disclosure is also "law" for these purposes: it is a published statement, contained in publicly accessible court judgments).

147. There is no merit in the criticism that the Disclosure or Code are *"obscurely drafted"* or *"vague"* for any of the reasons set out at §248(2)-(4) of the 10 HR Obs in Reply:

(1) It is entirely clear from the Disclosure/Code that the terms "request" and "receipt" would together cover all the scenarios where the relevant Intelligence Services may access foreign intercept. That would include access to databases. This alleged "obscurity" was not raised by 10 HR in the Liberty proceedings: no doubt, because it was not one that realistically arose.
(2) The concepts of "analysed" and "unanalysed" are also sufficiently clear (§248(3)). They are ordinary English words, which require no further definition. Material which has been automatically scanned and selected, but which has not been examined, is "unanalysed"; and material which has been examined, and conclusions drawn about it in the form of a report or analysis, is "analysed".
(3) It is wrong to suggest that there is no protection for communications data (§248(4)). As set out at §12.6 of the Code, where communications content or communications data (and whether or not the data is associated with the content of communications) are obtained in circumstances where the material identifies itself as the product of an interception, it must be subject to the same internal rules and safeguards that apply to the same categories of content or data when they are obtained directly by the intercepting agencies as a result of interception under RIPA.

148. As to the third argument, neither "prior independent authorisation" nor a requirement for "reasonable suspicion" are requirements of the s.8(4) Regime, for reasons set out below. So *a fortiori,* they cannot be requirements of the Intelligence Sharing Regime. In any event, there could be no sensible application of "reasonable suspicion" or "prior authorisation" requirements to circumstances where the Intelligence Services received unsolicited intercept material from a foreign state.

***The "necessity" test***

149. No separate question of "necessity" arises with regard to the Intelligence Sharing Regime under Article 8 or Article 10 ECHR, distinct from the issue whether the regime is "in accordance with the law". If the regime itself is "in accordance with the law" (as it is), any issue of necessity would arise only on the individual facts concerning any occasion where intelligence was shared,

since the sharing of intelligence may obviously be necessary and proportionate in some cases, but not others[91]. However, (i) the BBW Applicants do not allege that their intelligence was in fact shared by the US authorities with the Intelligence Services, and since they brought no complaint to the IPT, no investigation has been made into any such allegation; (ii) the IPT investigated the allegation by the 10 HR applicants that there had been sharing of their data in breach of the necessity test, and did not so find.

**Questions 3(b) and (c): are the acts of the Intelligence Services in relation to their own interception, search, analysis, dissemination, storage and destruction of interception data in respect of "external" communications and/or of interception data in respect of communications data in "accordance with the law" and "necessary" within the meaning of Articles 8 and 10?**

150. Questions 3(b) and (c) are dealt with compendiously below, because the s.8(4) Regime covers both intercepted communications and related communications data. The answer to both questions is "yes". (The regime under s.22 RIPA ("the s.22 Regime") is addressed briefly at the end of this section, in order to explain why the BIJ's contentions concerning it are misconceived).

**Four preliminary points**

151. Before addressing the application of the "in accordance with the law"/"prescribed by law" and "necessity" tests for the purposes of Articles 8 and 10 ECHR[92], four preliminary points should be noted:

(1) Some form of s. 8(4) Regime is a practical necessity, and the s. 8(4) Regime was designed on this basis, with the internet in mind.
(2) The existing ECtHR interception case law - and in particular *Weber*, *Liberty* and *Kennedy* - supports the Respondents' position that the "*in accordance with the law*" requirement is satisfied.
(3) The CJEU case law concerning data retention is not relevant to this issue.
(4) Contrary to the Applicants' case, it remains the case that intercepting communications (*i.e.* obtaining the content of communications) is in general more intrusive - and is thus deserving of greater protection - than obtaining communications data.

[91] Note however Farr §§15-25 regarding the general importance to the UK's national security interests of the intelligence it receives from the US authorities, which he states has led directly to the prevention of terrorist attacks and the saving of lives.

[92] As set out at §121 above with regards to the Intelligence Sharing Regime, the applicable test of foreseeability/accessibility does not differ, whether the analysis is undertaken under Article 8 or Article 10 ECHR. Indeed, the Court has frequently determined Article 8 and 10 complaints together, and stated that in light of the conclusions on one, it is unnecessary to address the other.

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

152. The s.8(4) Regime does not reflect some policy choice on the UK Government's part to undertake a programme of "*mass surveillance*", in circumstances where a warrant targeting a specific person or premises (as under s.8(1) RIPA) would be perfectly well suited to acquiring the external communications at issue. As the Commissioner has confirmed, and as follows from the facts at §§14-39 above, *there are no other reasonable means that would enable the Intelligence Services to have access to external communications that it is adjudged necessary to secure*. That is because (in simplified summary) (i) communications are sent over the internet in small pieces (i.e. "packets"), which may be transmitted separately, often by separate routes; (ii) in order to intercept a given communication of a target, while in transit over the internet, it is necessary to obtain all the "packets" associated with it, and reassemble them; and (iii) in order to reassemble the "packets", it is necessary to intercept the entirety of the contents of a bearer or bearers in order to discover whether any are intended for the target in question. In other words, the only practical way to find and reconstruct most external communication "needles" is to look through a communications "haystack".

153. The s. 8(4) regime was - to Parliament's knowledge – designed to accommodate the internet, and Parliament was made aware of the issue as noted above (see in particular Lord Bassam of Brighton's remarks in Parliament at **CB/38**). 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*": see the Report at §6.5.55[93]. The fact that there the internet has grown in scale does not render the safeguards under RIPA less relevant or adequate.

154. In addition, as Mr Farr explains and as the IPT accepted in the 5 December Judgment, 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: see Farr §§142-147. Those practical differences offer further justification for a regime of the form of the s. 8(4) Regime [Farr §149].

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

155. *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:

(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).
(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 manner that was not targeted at specific individuals and that might potentially extend to 10%

[93] See Annex 11

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).

(3) 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.

156. It follows that from the standpoint of the ECHR there is nothing in principle objectionable about an interception regime for external communications that is not targeted at specific individuals or premises; or a two-stage interception regime for external communications that involves an initial interception stage, followed by a selection stage which serves to identify a subset of that material that can thereafter be examined. This is unsurprising, not least given the points about the practical necessity of the s.8(4) Regime already made above.

157. As to *Liberty*:

(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*. 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). The subsequent publication of the RIPA Code showed (said the Court) that this was possible: see §68.

(2) 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. Indeed, it has been strengthened following *Liberty* by the changes made in January 2016.

(3) Further, the Court in *Liberty* did not conclude that Art. 8 required the UK Government to publish the detail of the Secretary of State's "*arrangements*" under s. 6 of the Interception of Communications Act 1985 (now ss. 15-16 of RIPA). Rather, it implicitly accepted that publication of full (rather than "certain") details would be likely to compromise national security. And since the Code reflects the Disclosure, it contains all of those parts of the Intelligence Services' internal arrangements which the IPT considered in the Liberty proceedings could safely be disclosed without damaging national security.

158. In *Kennedy* the ECtHR unanimously upheld the Art. 8-compatility 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*. Indeed, the Code has been significantly strengthened since *Kennedy,* including by the addition of provisions to strengthen the s.8(4) Regime safeguards in particular: so the fact that the ECtHR gave the RIPA regime the stamp of approval in *Kennedy* regarding s.8(1) warrants is a strong indicator that the same outcome should follow for the s.8(4) Regime.

***iii. The CJEU's case law concerning data retention is irrelevant.***

159. The Applicants place some reliance upon the CJEU's judgments in *Digital Rights Ireland C-293/12,* 2014/C 175/07, 8 April 2014[94] (*"Digital Rights"*)[95] and Joined Cases *Tele2 Sverige C-203/15* and *Watson & ors C-698/15*, "*Watson",* 21 December 2016 (**CB/57**). Both *Digital Rights* and *Watson* are immaterial to the questions before this Court.

160. *Digital Rights* and *Watson* were both preliminary references concerning the compatibility with EU law of requirements for communications services providers ("CSPs") to retain traffic and location data, so that it could be made available to national authorities[96]. The cases addressed among other matters the circumstances in which, and conditions under which, CSPs must grant competent national authorities access to retained traffic and location data in the context of criminal investigations. However, neither *Digital Rights* nor *Watson* was concerned with the activities of national authorities themselves in the sphere of national security, nor could they have been.

161. The EU may only act within the sphere of competencies conferred upon it by the Member States in the Treaties. Competencies not conferred upon the Union in the Treaties remain with Member States. Matters of Member States' national security are not conferred on the EU. On the contrary, they are positively identified as being the sole responsibility of Member States in Article 4(2) of the Treaty on European Union ("TEU")[97]. This issue, as to whether the EU has any competence in this sort of national security sphere, is the subject of the reference to the CJEU recently made by the IPT in the Privacy 2 Judgment (**CB/21**).

162. As appears from that judgment, there are live issues not merely about this foundational jurisdictional issue flowing from Article 4(2) TEU. There is also a set of live issues as to

---

[94] See e.g. BBW Update Submissions, §17.

[95] See Annex 16, **CB/54**.

[96] *Digital Rights Ireland* was a preliminary reference concerning the validity of Directive 2006/24/EC on Data Retention (see Annex 48), a EU-wide harmonisation measure adopted pursuant to Article 95 EC. The Directive required CSPs in the EU to retain all customer data for a period of not less than 6 months, and up to 2 years, so that it could be made available to law enforcement authorities. The Directive contained no substantive safeguards at all circumscribing access to or use of that communications data. *Watson* concerned (i) the compatibility with EU law of a requirement for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users, so that it could be made available to the national authorities for the purposes of fighting crime (such a requirement existing in Swedish law for the purposes of implementing Directive 2006/24/EC); and (ii) the issue whether *Digital Rights* laid down mandatory requirements of EU law applicable to Member States' domestic regimes governing access to data retained by CSPs in accordance with national legislation.

[97] Articles 4(1) and (2) TEU provide as follows (underlining added):
*"1. In accordance with Article 5, competencies not conferred upon the Union in the Treaties remain with the Member States.*
*2. The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State."*

whether (a) the CJEU was even purporting to consider or address the nature of any safeguards it considered necessary in a context involving state activity in the protection of national security (the Government's case is that the CJEU was not purporting to do so); and (b) how the sorts of safeguards the CJEU considered in those cases could conceivably be considered appropriate, let alone necessary, in such a context. The Court is invited to read the Privacy 2 Judgment in particular in relation to point (b).

163. It is evident that the IPT (with its intimate knowledge of the work of the Intelligence Services and the nature and operation of the safeguarding regimes) had the gravest doubts as to whether those sorts of safeguards could appropriately be applied into the very different national security context before it: see especially §§54-69. That was particularly so given their conclusion that, if the *Watson* requirements did apply "*to measures taken to safeguard national security, in particular the [bulk communications data] regime, they would frustrate them and put the national security of the United Kingdom, and, it may be, other Member States, at risk"* (§69).

164. It is to be noted finally in this respect that this Court has had the opportunity over the years on many occasions to consider the necessary safeguards to be applied in similar contexts with potentially profound impacts on national security. Those Convention safeguards, as appears clearly from the Court's jurisprudence, sit within and are to be considered as part of the Convention scheme as a whole. That scheme represents a balance between private interests and the interests of the general community; and it involves a recognition of the proper national responsibility, subject to oversight by the Court, for the protection of the State's citizens. Given that long experience, it is unsurprising that the CJEU has repeatedly (and correctly under the EU Treaties including the Charter) emphasised that, in summary, it takes its lead on these sorts of issues from this Court's jurisprudence.

***iv. Intercepting communications is in general more intrusive than obtaining communications** data*

165. The ECtHR recognised in §84 of *Malone* that it is less intrusive to obtain communications data than the contents of communications. 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. The Applicants seek to dispute this, in particular by reference to the possibility of aggregating communications data. (See *e.g.* BBW Update Submissions at §§18-20 and Brown w/s §§8-13[98]).

166. 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. Nevertheless, it is possible that aggregating communications

[98] **CB/4**.

data may in certain circumstances (and, potentially, with the addition of further information that is not communications data)[99] 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-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.

167. Further, as set out below at §194(1), any information from or about a communication that is not "related communications data" for the purposes of the statutory definition in ss.20/21 RIPA falls to be treated as content, not communications data, under the s.8(4) Regime; and "related communications data" is a limited subset of metadata as a whole.

**The s.8(4) Regime is "in accordance with the law"**

168. The Art. 8/10 interferences in question have a basis in domestic law, namely the s. 8(4) Regime. Further, the "accessibility" requirement is satisfied in that RIPA is primary legislation[100] and the Code is a public document, and insofar as the operation of the s. 8(4) Regime is further clarified by the Commissioner's Reports, those are also public documents.

169. As regards the foreseeability requirement, account must be taken - as in the case of the Intelligence Sharing Regime - of the special context of secret surveillance, and the well-established principle that the requirement of foreseeability: "*...cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly*." (*Weber*, at §93. See also *e.g.* §67 of *Malone*.) This fundamental principle applies both to the interception of communications (so as to obtain intercepted material, *i.e.* the content of communications) and to the obtaining of related communications data (*i.e.* data that does not include the content of any communications). However, in other respects, the precise requirements of foreseeability differ for the interception of communications, on the one hand, and the obtaining of related communications data, on the other, as the former is more intrusive than the latter.

[99] See the example noted at Brown w/s §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).
Moreover, a significant number of the examples given by the Applicants concerning the aggregation of communications data would be inapplicable to GCHQ and/or unlawful having regard to the applicable statutory framework.

[100] Insofar as the S. 8(4) Regime incorporates parts of the Intelligence Sharing and Handling regime, that also is "accessible".

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

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

> *"[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).

171. The *Liberty, Kennedy* and *Zakharov* cases make clear that it is not necessary that every provision / rule be set out in primary legislation.

172. 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*". The *Weber* safeguards are thus a facet of the more general principle that there must be adequate and effective guarantees against abuse. Accordingly, in determining whether the domestic safeguards meet the minimum standards set out in §95 of *Weber*, account should be taken of all the relevant circumstances, including: "*the authorities competent to ... supervise [the measures in question], and the kind of remedy provided by the national law ...*" (*Association for European Integration and Human Rights v Bulgaria*, App. 62540/00, 28 June 07, §77.)

173. Thus, as in the case of the Intelligence Sharing and Handling Regime, the Government relies on the relevant oversight mechanisms, namely the Commissioner, the ISC and the Tribunal. All the points already made at §§52-81 above as to the wide scope, independence and effectiveness of those mechanisms apply equally in this context.

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

174. This requirement is satisfied by s. 5 of RIPA, which defines the purposes for which the Secretary of State can issue an interception warrant, provided that it is necessary and appropriate to do so, as read with the relevant definitions in s. 81 of RIPA and §§6.11-6.12 of the Code[101]. This follows, in particular, from a straightforward application of §159 of *Kennedy,* and §133 of

[101] By section 5(2) RIPA, the Secretary of State may not issue a warrant unless he believes that the warrant is "*necessary on grounds falling within subsection (3)*", and that the conduct authorised by the warrant is proportionate. A warrant is necessary on grounds falling within s.5(3) only if it is necessary (a) in the interests of national security; (b) for the purpose of preventing or detecting serious crime; or (c) for the purpose of safeguarding the economic well-being of the UK, in circumstances appearing to the Secretary of State to be relevant to the interests of national security. The terms "*preventing*", "*detecting*" and "*serious crime*" are all defined in s.81 RIPA.

*RE v United Kingdom*. (See further below at §§229-234 as regards the meaning of "national security").

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

175. 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).

176. As regards the *interception* stage:

(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.
(2) The term "*communication*" is sufficiently defined in s. 81 of RIPA[102]. The term "*external communication*" is sufficiently defined in s. 20 RIPA and §5.1 of the Code (see §§221-228 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*".
(3) Further, the s. 8(4) regime does not impose any express limit on the number of external communications which may fall within "*the description of communications to which the warrant relates*" in s. 8(4)(a). As is made clear in numerous public documents, a s. 8(4) warrant may in principle result in the interception of "*substantial quantities of communications…contained in "bearers" carrying communications to many countries"*[103]. Similarly, during the Parliamentary debate on the Bill that was to become RIPA, Lord Bassam referred to intercepting the whole of a communications "*link*"[104]).

---

[102] "*Communication*", as defined in s.81 RIPA, means (as far as material) *"anything comprising speech, music, sounds, visual images or data of any description"* and *"signals serving either for the impartation of anything between persons, between a person and thing or between things or for the actuation or control of any apparatus."*

[103] See the 5 December Judgment at §93. See too, for example, the ISC Report, **CB/47**.

[104] See the discussion of the Bill in the House of Lords on Wednesday 12 July 2000 at Annex 26, **CB/38**. In that debate, Lord Bassam (as the Government Minister sponsoring the Bill) stated:
*"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 at 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 these two foreign countries. Such a link should clearly be treated as being external, yet it would contain at least this one internal communication. There is no way of filtering that out without intercepting the whole link, including the internal communication.*
*Even after interception, it may not be practicably possible to guarantee to filter out all internal messages. 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. Without this information it will not be possible to distinguish internal messages from external. In some cases it may not be possible even if this information is available. For example, a message between two foreign registered mobile phones, if both happened to be roaming in the UK, would be an internal communication, but there would be nothing in the message to indicate that."*

(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[105], 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). This point was also made clear to Parliament (see footnote 106 below, and the remarks of Lord Bassam) and it has in any event been publicly confirmed by the Commissioner (see §36 above).

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

177. As regards the *selection* stage:

(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) HRA) it is proportionate to do so in the particular circumstances of the case. See s.16(1) RIPA.

(2) The categories of communications set out in the Secretary of State's certificate must relate directly to the intelligence-gathering priorities set by the Joint Intelligence Council and agreed by the National Security Council (see the Code at §6.14, and see too for confirmation of the factual position the ISC Report at §100, third bullet point).

(3) The Commissioner confirmed in his 2013 Report that the certificate is regularly reviewed and subject to modification by the Secretary of State[106]. The Code also makes clear that any changes to the description of material specified in the certificate must be reviewed by the Commissioner: see Code, §6.14.

(4) Material will only fall within the terms of the certificate insofar as it is of a category described therein; and insofar as the examination of it is necessary on the grounds in s. 5(3)(a)-(c) RIPA. Those grounds are themselves sufficiently defined for the purposes of the foreseeability requirement. See §159 of *Kennedy*[107] (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*"). See further at §§229-232 below as regards the meaning of "national security".

(5) Further, s. 16(2) 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

---

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

[106] See the 2013 Report at §6.5.43, Annex 11, **CB/35**, and see too Farr w/s §80, Annex 3, **CB/9**.

[107] The Applicants argue that the meaning of "*serious crime*" is insufficiently clear; but at §159 of *Kennedy* the ECtHR observes that RIPA itself contains a clear definition both of "*serious crime*" and what is meant by "*detecting*" serious crime: see section 81 RIPA.

listened to according to a factor which is referable to an individual who is known to be for the time being in the British Islands and which has as its purpose, or one of its purposes, the identification of material contained in communications sent by him or intended for him. Thus, by way of example, intercepted material could not in general be selected to be listened to by reference to a UK telephone number. Before this could be done, it would be necessary for the Secretary of State to certify that the examination of a person's communications by reference to such a factor was necessary; any such certification would need to reflect the NSC's "Priorities for Intelligence Collection"[108]. Moreover, the system ensures that, if is subsequently discovered that an individual is actually in the UK, when previously that was not known, the Intelligence Services must cease all action at that point[109].

178. The above controls in s.16 RIPA (and the HRA) constrain all access at the selection stage, irrespective whether such access is requested by a foreign intelligence partner. Further, any such access requested by a foreign partner, 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[110].

179. The above provisions do not permit indiscriminate trawling, as the Commissioner has publicly confirmed (see his 2013 Annual Report at §6.5.43, **CB/35**).

180. In the light of the above and, having regard - again - to the principle that an individual should not be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly and to the available oversight mechanisms, 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 IPT was right so to conclude in the Liberty proceedings.

*(c) Limits on the duration of telephone tapping*

181. The s. 8(4) Regime makes sufficient provision for the duration of any s.8(4) warrant, and for the circumstances in which such a warrant may be renewed: see §161 of *Kennedy,* and the specific provisions for renewal of a warrant contained in §§6.22-6.24 of the Code[111]. Thus, under the Code, the application for renewal must be made to the Secretary of State; must contain all the

[108] See the Code, §6.14. The Applicants complain that "*no guidance is given as to how the Secretary of State will assess such necessity*" (see Application, §151). However, that contention is wrong. See §7.19 of the Code, Annex 10, **CB/33**.

[109] See e.g. §112(iv) of the ISC Report at Annex 13, **CB/47**.

[110] Contrast §161 of the BBW Application, which wrongly asserts that there is *"no restriction on search terms being specified by foreign intelligence partners such as the NSA or search results being shared with them."*

[111] Note too that the provisions for renewal of a warrant contained in §§6.22-6.24 of the Code are at least as detailed as those found lawful by the ECtHR in relation to the renewal of warrants for covert surveillance under Part II RIPA, considered in *RE v United Kingdom*: see *RE* at §137. Contrast §162 of the Application, which wrongly states that chapter 6 of the Code does not *"impose any limits on the scope or duration of warrants".*

detailed information set out in §6.10 of the Code; must give an assessment of the value of interception to date; and must state why interception continues to be necessary for one or more of the statutory purposes in s.5(3) RIPA, and proportionate.

182. No s.8(4) warrant may be renewed unless the Secretary of State believes that the warrant continues to be necessary on grounds falling within s.5(3) RIPA: see s.9(2) RIPA. Further, by s.9(3), the Secretary of State must cancel a s.8(4) warrant if he is satisfied that it is no longer necessary on those grounds. Detailed provision for the modification of warrants and certificates is made by s.10 RIPA.

183. §6.27 of the Code requires records to be kept of all renewals and modifications of s.8(4) warrants/certificates, and the dates on which interception was started and stopped, thus enabling the Commissioner to have the appropriate oversight.

184. The possibility that a s. 8(4) warrant might be renewed does not alter the analysis. 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.

185. Moreover, for completeness, it should be noted that these are not circumstances in which warrants will *"always be renewed",* contrary to the Applicants' assertion. That assertion is directly contrary to §6.7 of the Code (and Farr §154, **CB/9**). The Code requires regular surveys of relevant communications links to identify those which are most likely to contain external communications meeting the descriptions of material certified by the Secretary of State under s.8(4) RIPA (and thus interception only of those particular links).

*(d)-(e) 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*

186. 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 (§7.7 of the Code).

187. As regards the intercepted material that can be read, looked at or listened to pursuant to s. 16 (and the certificate in question), the applicable regime (see §§2.74-2.87 of the BBW Observations) is well sufficient to satisfy the fourth and fifth foreseeability requirement in §95 of *Weber*. See §163 of *Kennedy*, and the following matters (various of which add to the safeguards considered in *Kennedy*):

(1) Material must generally be selected for possible examination applying search terms, by equipment operating automatically for that purpose (so that the possibility of human error or deliberate contravention of the conditions for access at this point is minimised). Moreover,

the person proposing to select it for examination must create a record setting out why access to the material is required and proportionate, and consistent with the applicable certificate, and stating any circumstances that are likely to give rise to a degree of collateral infringement of privacy, and any measures taken to reduce the extent of that intrusion. See the Code, §§7.14-7.16.

(2) The Code affords further protections to material accessed under the s.8(4) Regime at §§7.11-7.20. Thus, material should only be read, looked at or listened to by authorised persons receiving regular training in the operation of s.16 RIPA and the requirements of necessity and proportionality; systems should to the extent possible prevent access to material without the record required by §7.16 of the Code having been created; the record must be retained for the purposes of subsequent audit; access to the material must be limited to a defined period of time; if access is renewed, the record must be updated with the reasons for renewal; systems must ensure that if a request for renewal of access is not made within the defined period, no further access will be granted; and regular audits, including checks of the particular matters set out in the Code, should be carried out to ensure that the requirements in s.16 RIPA are met.

(3) 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 §7.6 of the Code as regards copying and §7.7 of the Code as regards storage (the latter being reinforced by the seventh data protection principle).

(4) Further, s. 15(2) RIPA 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[112]). 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 §§7.4 and 7.5 of the Code. The obligations imposed by those provisions of the Code include that where intercepted material is disclosed to the authorities of a foreign state, the agency must take reasonable steps to ensure that the authorities have and will maintain the necessary procedures to safeguard the intercepted material, and to ensure that it is disclosed, copied, distributed and retained only to the minimum extent necessary (and it must not be further disclosed to the authorities of a third country unless explicitly agreed).

(5) 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, disclosure 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 is rendered criminal by s. 1(1) of the OSA.

---

[112] *"(2) The requirements of this subsection are satisfied in relation to the intercepted material and any related communications data if each of the following-*
*(a) The number of persons to whom any of the material or data is disclosed or otherwise made available,*
*(b) The extent to which any of the material or data is disclosed or otherwise made available,*
*(c) The extent to which any of the material or data is copied, and*
*(d) The number of copies that are made,*
*Is limited to the minimum that is necessary for the authorised purposes."*

188. As already noted, the detail of the s. 15 and s.16 arrangements is kept under review by the Commissioner.

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

189. S. 15(3) of RIPA and §§7.8-7.9 of the Code (including the obligation to review retention at appropriate intervals, and the specification of maximum retention periods for different categories of material, which should normally be no longer than 2 years) make sufficient provision for this purpose. See *Kennedy* at §§164-165 (and note that further safeguards in §7.9 of the Code, including the specification of maximum retention periods, have been added to the Code since *Kennedy*). Both s. 15(3) and the Code are reinforced by the fifth data protection principle.

*Conclusion as regards the interception of communications*

190. 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). The IPT was right so to conclude in the Liberty proceedings.

***(2) Foreseeability of the acquisition of related communications data under the s. 8(4) Regime***

191. *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*). The list of safeguards in §95 of *Weber* has never been applied by the ECtHR to powers to acquire communications data. 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, as 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.

192. Moreover, the ECtHR has specifically not applied the *Weber* requirements to other types of surveillance. For example, in *Uzun v Germany* app. No. 35623/05, 2 September 2010, the ECtHR specifically declined to apply the "rather strict" standards in *Weber* to surveillance via GPS installed in a suspect's car, which tracked his movements. That sort of tracking information is precisely analogous to the type of information obtained from traffic data (i.e. obtained from a subset of related communications data). Thus, the fact that the Court has declined to apply *Weber* in such circumstances is a powerful indicator that the *Weber* criteria should not apply to the acquisition of related communications data under the s.8(4) Regime.

193. Instead of the list of specific safeguards in *e.g.* §95 of *Weber*, the test should therefore be 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*).

194. The s. 8(4) Regime satisfies this test as regards obtaining and use of related communications data:

(1) As a preliminary point, the controls within the s.8(4) Regime for "related communications data" - as opposed to content - apply to only a limited subset of metadata. "Related communications data" for the purposes of the s.8(4) Regime has the statutory meaning given to it by ss.20 and 21 RIPA[113]. That meaning is not synonymous with, and is significantly narrower than, the term "metadata", used by the Applicants in this context. The Applicants define "metadata" as "*structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource"* (see BBW Application, §21). On that definition, much "metadata" amounts to the content of communications for the purposes of the s.8(4) Regime, not related communications data (since all information that is not "related communications data" must be treated as content). For instance, email addresses or telephone numbers from the body of a communication would generate "metadata"; but would be "content" for the purposes of the s.8(4) Regime. The language or format used for a communication would be "metadata"; but again, "content" for the purposes of the s.8(4) Regime.

(2) The s. 8(4) Regime is sufficiently clear as regards the circumstances in which the Intelligence Services can **obtain** related communications data. See §§174-176 above, which applies equally here.

(3) Once obtained, **access** to any related communications data must be necessary and proportionate under s. 6(1) of the HRA, and will be subject to the constraints in ss.1-2 of the SSA and ss. 1-2 and 3-4 of the ISA. Any access by any foreign intelligence partner at this stage would be constrained by ss. 15(2)(a) and 15(2)(b) of RIPA (as read with s. 15(4)); and, as it would amount to a disclosure by the Intelligence Service in question to another person

---

[113] By section 20 RIPA: *""Related communications data", in relation to a communication intercepted in the course of its transmission by means of a postal service or telecommunication system, means so much of any communications data (within the meaning of Chapter II of this Part) as-*

*(a) Is obtained by, or in connection with, the interception; and*

*(b) Relates to the communication or to the sender or recipient, or intended recipient, of the communication".*

By section 21(4) RIPA:

*"In this Chapter "communications data" means any of the following-*

*(a) Any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;*

*(b) Any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person-*

*i. Of any postal service or telecommunications service; or*

*ii. In connection with the provision to or use by any person of any telecommunications service, or any part of a telecommunication system;*

(c) *Any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service."*

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. Further, and importantly, the safeguards in §§7.1-7.10 of the Code (supplementing the s.15 "arrangements") apply here, as they do to communications. Those impose obligations including that where intercepted material is disclosed to the authorities of a foreign state, the agency must take reasonable steps to ensure that the authorities have and will maintain the necessary procedures to safeguard the intercepted material, and to ensure that it is disclosed, copied, distributed and retained only to the minimum extent necessary (and it must not be further disclosed to the authorities of a third country unless explicitly agreed).

(4) Given the constraints in ss. 15 of RIPA and s. 6(1) of the HRA, communications data cannot 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 discovering 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).

195. 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:

(1) 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)). Related communications data is a significant resource in this regard.

(2) 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*".

196. The regime equally contains sufficient clear provision regarding the subsequent **handling, use and possible onward disclosure** by the Intelligence Services of related communications data. Section 15 RIPA and the safeguards in §§7.1-7.10 of the Code apply equally here. See §187 above.

197. 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 each of those requirements so imposed

given §194 above (and, as regards the limits on the duration of s. 8(4) warrants, §§181-185 above).

***Further issues regarding foreseeability/accessibility***

198. The Applicants raise certain specific complaints about the foreseeability of the s.8(4) Regime, each of which is addressed below in order to explain why it does not affect the general conclusion on foreseeability/accessibility set out above. They are:

(1) The lack of need for reasonable suspicion.
(2) The fact that there is no requirement for prior independent authorisation of warrants, which is said both to be generally objectionable, and specifically objectionable in the case of journalists/NGOs;
(3) The fact that there is no requirement for subsequent notification;
(4) The supposedly *"expansive"* definition of "external communications";
(5) The breadth of the concept of "national security" and/or "serious crime".

*No need for reasonable suspicion*

199. The Applicants now contend purportedly on the basis of *Zakharov* and *Szabo* that no interception should be carried out at all without "reasonable suspicion". In other words, all individuals should be individually identified and targeted before any interception takes place. This is not what the law requires. It is not mandated by Article 8 ECHR, it is not a proper analysis of *Zakharov* or *Szabo,* and it would in practice denude the interception of communications under the s.8(4) Regime of a very large portion of its utility, thereby endangering the lives of UK citizens.

200. The true principle to be derived from the authorities on Article 8 is that any interception of and access to communications must be necessary and proportionate, and must satisfy the *Weber* criteria, which the s.8(4) Regime does: see §§161-197 above. Any attempt to frame a narrower rule is contrary to the whole thrust of the Court's case law, which permits "strategic monitoring": see *Weber,* where the challenge to the German state's regime in this respect was not only dismissed, but declared manifestly ill-founded. The Applicants impermissibly elevate the Court's particular findings on the specific facts of certain cases into statements of general principle.

201. In particular, the Applicants rely on *Zakharov* to contend that "reasonable suspicion" against an individual is a necessary precondition for any surveillance, because the Court found that *"the authorisation authority's scope of review… must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting the person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures…"*: *Zakharov*, §260.

202. That finding at §260 of *Zakharov,* however, must be seen in its context. It concerned the sufficiency of the authorisation authority's scope of review, where the issue was the propriety of the intelligence agency's request to perform a search operation targeting the communications of a specific individual (see e.g. §§38 and 44 of the judgment). The Court accepted that the requirement for prior judicial authorisation in Russian law was an important safeguard, but found that it was insufficient in the circumstances, because the domestic court's scrutiny was limited. The domestic court had no power to assess whether there was a sufficient factual basis for targeting the individual concerned: see §§260-261. Moreover, there was no effective *post facto* judicial scrutiny either: §298. Thus, the totality of the safeguards did not provide adequate and effective guarantees against abuse: §302.

203. In short, the context in *Zakharov* concerned the nature of the available safeguards, where a particular individual had already been targeted; and unsurprisingly, the Court considered that it was important for those safeguards to include effective independent judicial oversight of that targeting decision, capable of assessing its merits.

204. Nothing in *Zakharov* either states or implies that, in order for there to be sufficient safeguards against abuse, any target of surveillance must always be identified in advance on the basis of reasonable suspicion. Rather, the true position on the basis of the Court's jurisprudence is that:

(1) It is the totality of safeguards against abuse within the system that is to be considered. See e.g. *Zakharov* at §§257, 270-271.
(2) Where a decision has been made to target a particular individual, it will be necessary for a judicial authority to be able to review that decision on its merits (i.e. to determine not simply whether it was taken in accordance with proper procedures, but to assess whether it was necessary and proportionate). See *Zakharov*.
(3) However, such judicial oversight can be either *ex ante* or *post facto*: see e.g. *Szabo* at §77, *Kennedy* at §167.
(4) The s.8(4) Regime provides such oversight. The IPT is able to, and will, examine the necessity and proportionality of any interception or examination of the complainant's communications, with the benefit of full access to the evidence. See §§58-66 above.

205. As to the Applicants' reliance on *Szabo*, as the Applicants themselves accept (see §186(2) of the 10 HR Obs in Reply), the Fourth Section's observations at §71 of the judgment were in the context of its proportionality assessment and whether the type of "secret surveillance" which had been undertaken by the TEK had been demonstrated as necessary and proportionate. Again, these observations have to be seen in the context of a regime which allowed ordering of interception entirely by the Executive, with no assessment of necessity, with potential interception of individuals outside the operational range, and in the absence of any effective remedial or judicial measures.

206. For the reasons explained at §§14-30 above, the conclusions of the ISC, IPT, Anderson Report and Bulk Powers Review all demonstrate that the bulk interception powers in the s.8(4)

regime are necessary and proportionate, even where the intelligence services are searching for the communications of individuals who have not already been identified as a target and in order to identify threats to the UK. That does not "obviate" any meaningful assessment of proportionality, as e.g. the Bulk Powers Review and the case studies referred to therein amply demonstrate.

*No prior independent authorisation of warrants*

207. Just as in *Kennedy*, the extensive oversight mechanisms in the s.8(4) Regime offer sufficient safeguards to render the regime in accordance with the law, without any requirement for independent (still less, judicial) pre-authorisation of warrants.

208. **First,** and as the Applicants rightly recognise, the ECtHR's case law does not require independent authorisation of warrants as a precondition of lawfulness, provided that the applicable regime otherwise contains sufficient safeguards. Given the possibilities for abuse inherent in a regime of secret surveillance, it is on the whole in principle desirable to entrust supervisory control to a judge: but such control may consist of oversight after rather than before the event. Extensive *post factum* judicial oversight can counterbalance absence of pre-authorisation. See *Klass v Germany*, 6 September 1978, Series A no.28 at §51, *Kennedy* at §167, and most recently, the detailed consideration of the issue in *Szabo and Vissy v Hungary* app.37138/14 (12 January 2016) at §77[114].

209. The Applicants now rely upon *Digital Rights* and *Watson* in this respect. However, neither of those cases lays down definitive mandatory requirements in the present context; neither purports to extend principles under Article 8 (or 10) ECHR; and in any event, as already explained above, neither applies (or could apply) to the acts of Member States in the field of national security.

210. **Secondly,** the extensive independent (including judicial) *post factum* oversight of secret surveillance under the s.8(4) Regime compensates for the fact that s.8(4) warrants are authorised by the Secretary of State, rather than by a judge or other independent body.

211. The very same observations made by the ECtHR at §167 of *Kennedy,* in which the Court found that the oversight of the IPT compensated for the lack of prior authorisation, apply equally here:

> *"…the Court highlights the extensive jurisdiction of the IPT to examine any complaint of unlawful interception. Unlike in many other domestic systems, any person who suspects that his communications have been or are being intercepted may apply to the IPT. The jurisdiction of the IPT does not, therefore, depend on notification to the interception subject that there has been an*

[114] To the extent that *Iordachi v Moldova* app.25198/02, 10 February 2009 implies at §40 that there must in all cases be independent prior authorisation of warrants for interception, it is inconsistent with the later cases of *Kennedy* and *Szabo,* and cannot stand with the general thrust of the ECtHR's case law.

*interception of his communications. The Court emphasises that the IPT is an independent and impartial body, which has adopted its own rules of procedure. The members of the tribunal must hold or have held high judicial office or be experienced lawyers. In undertaking its examination of complaints by individuals, the IPT has access to closed material and has the power to require the Commissioner to provide it with any assistance it thinks fit and the power to order disclosure by those involved in the authorisation and execution of the warrant of all documents it considers relevant. In the event that the IPT finds in the applicant's favour, it can, inter alia, quash any interception order, require destruction of intercept material and order compensation to be paid. The publication of the IPT's legal rulings further enhances the level of scrutiny afforded to secret surveillance activities in the United Kingdom."*

212. Moreover, the following additional points about the applicable *post factum* independent oversight should also be made:

(1) The IPT is not only in principle but in fact an effective system of oversight in this type of case, as the Liberty proceedings indicate: see §§40-51 above.
(2) The Commissioner oversees the issue of warrants under the s.8(4) Regime as part of his functions, and looks at a substantial proportion of all individual warrant applications in detail. See §§67-77 above.
(3) The ISC also provides an important means of overseeing the s.8(4) Regime as a whole, and specifically investigated the issuing of warrants in the ISC Report (see the report, pp.37-38, **CB/47**).

*Is the position any different under Article 10 as concerns journalists/NGOs?*

213. Prior authorisation is the only respect in which the Applicants contend that the position as regards the "in accordance with law" test may differ under Article 10 from that under Article 8, and in respect of which they assert that their identity as journalists/NGOs may be material to the analysis.

214. However, there is no authority in the Court's case law[115] for the proposition that prior judicial (or independent) authorisation is required for the operation of a strategic monitoring regime such as the s.8(4) Regime, by virtue of the fact that some journalistic (or NGO) material may be intercepted in the course of that regime's operation. On the contrary, the Court has drawn a sharp and important distinction between the strategic monitoring of communications and/or communications data, which may inadvertently "sweep up" some journalistic material; and measures that target journalistic material, particularly for the purposes of identifying sources, where prior independent authorisation will be required. See *Weber* at §151, and contrast *Sanoma Uitgevers BV v The Netherlands* app. no. 38224/03, 14 September 2010, and *Telegraaf Media v The Netherlands*[116].

[115] Or the domestic case law for that matter.
[116] In *Weber* at §151 the Court stated: *"The Court observes that in the instant case, strategic monitoring was carried out in order to prevent the offences listed in s.3(1). It was therefore not aimed at monitoring journalists; 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 cannot, therefore, be classified as particularly serious."*

215. Moreover, even if it were considered desirable in principle, a requirement of prior judicial authorisation for journalistic material in the operation of the s.8(4) Regime would be nugatory, as observed by the IPT in the Liberty proceedings in the 5 December judgment[117], at §151:

> *"We are in any event entirely persuaded that this, which is not of course a case of targeted surveillance of journalists, or indeed of NGOs, is not such an appropriate case, particularly where we have decided in paragraph 116(vi) above, that the present system is adequate in accordance with Convention jurisprudence without prior judicial authorisation. In the context of the untargeted monitoring by s.8 (4) warrant, it is clearly impossible to anticipate a judicial pre-authorisation prior to the warrant limited to what might turn out to impact upon Article 10. The only situation in which it might arise would be in the event that in the course of examination of the contents, some question of journalistic confidence might arise. There is, however, express provision in the Code (at paragraph 3.11), to which we have already referred, in relation to treatment of such material."*

216. Those observations are clearly correct. A requirement of prior judicial authorisation in respect of journalistic or NGO material under a regime of strategic (non-targeted) monitoring such as the s.8(4) Regime would simply make no sense. All that a Judge could be told is that there was a possibility that the execution of the warrant might result in the interception of some confidential journalistic/NGO material (along with other categories of confidential material). In the event that any such material was selected for examination the relevant provisions of the Code would apply.

*No requirement for subsequent notification*

217. The 10 HR Applicants now assert on the basis of *Szabo* that there should be a minimum requirement of subsequent notification to individuals, when this no longer jeopardises the purpose of surveillance. This was not an argument that 10 HR raised in the IPT, and it is wrong.

218. As set out above, the *Szabo* decision has to be read in the context of a regime which contained no meaningful safeguards. The Court reached its determination on the basis that there was a failure to comply with the *Weber* criteria, and it was unnecessary for the Court to embark on the question whether enhanced guarantees were necessary (§70). Accordingly, the Court did not purport to lay down further minimum requirements over and above *Weber*; and there was no indication in §86 that subsequent notification of surveillance measures was such a requirement. As the Court noted at §86, it was the *combination* of a complete absence of safeguards plus a lack of notification which meant that the regime could not comply with Art. 8 ECHR.

219. The work of the Intelligence Services must be conducted in secret if it is to be effective in achieving its aims. The value of intelligence work often relies on an identified target not knowing that his activities have come to the attention of the agencies, and/or not knowing what level of access to his activities the agencies have achieved. The requirement to notify a suspect of the use of bulk data tools against him, simply on the grounds that investigations have been concluded, would fundamentally undermine the work of the agencies. It may also threaten the lives of covert

[117] See Annex 15, **CB/14**

human intelligence sources close to him, such as a source who has provided the target's telephone number or email address to the Intelligence Services. Moreover, such a notification requirement may be wholly impractical in the case of many of the targets of interception under the s.8(4) Regime, who will be based abroad (often in locations lacking State control), and whose personal details may be unknown or imperfectly known.

220. The Government notes that this is wholly consistent with the reasoning of the Court in *Klass v Germany* at §58:

> *"In the opinion of the Court, it has to be ascertained whether it is even feasible in practice to require subsequent notification in all cases.*
>
> *The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. Furthermore, as the Federal Constitutional Court rightly observed, such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents. In the Court's view, in so far as the 'interference' resulting from the contested legislation is in principle justified under Article 8 (2) (see para. 48 above), the fact of not informing the individual once surveillance has ceased cannot itself be incompatible with this provision, since it is this very fact which ensures the efficacy of the 'interference'...*"

*The definition of "external communications"*

221. The Applicants complain about the supposedly "expansive" way in which the Government applies the definition of "external communications" in s.20 RIPA, by reference to Farr §§129-138, and contend that this "expansive" interpretation is insufficiently accessible (hence, does not meet the "in accordance with the law" requirement). This complaint lacks merit (and an identical complaint was rejected by the IPT – see the 5 December Judgment, §§93-101).

222. **First**, the definition of "external communications" in s.20 RIPA and the Code is itself a sufficiently clear one[118]. The Applicants and Government are agreed that it draws a distinction between communications that are both sent and received within the British Islands (however they are routed), and communications that are not both sent and received within the British Islands; and the focus of the definition is upon the ultimate sender, and ultimate intended recipient, of the communication.

223. Further, although the ways in which the internet may be used to communicate evolves and expands over time, the application of the definition remains foreseeable. For instance, 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. See Farr §§133-

[118] 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 §6.5 of the Code (which explains inter alia that communications both sent and received in the British Islands are not external, merely because they pass outside the British Islands en route).

137[119], **CB/9**. 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[120].

224. However, the Applicants 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:

(1) 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 it is in practice inevitable that, when intercepting material at the level of communications links, both "*internal*" and "*external*" communications will be intercepted.

(2) The distinction between external and internal communications offers an important safeguard at a "macro" level, when it is determined what bearers should be targeted for interception under the s. 8(4) Regime. When deciding whether to sign a warrant under s. 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 "external communication" in s. 20 of RIPA and the Code.

225. 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.

226. **Thirdly**, the safeguards in ss. 15 and 16 RIPA (as elaborated in the Code) apply to internal

[119] The Applicants imply that the Code should explain how the distinction between "external" and "internal" communications applies to various modern forms of internet use (see e.g. the complaint at BBW Update Submissions, §56, that the Code of Practice is *"otherwise silent on the application of RIPA to the internet"*). The difficulty with this submission is if it were correct, then 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 in §§224-227 below) pointless; and the "in accordance with the law" test under Art. 8 cannot conceivably impose such a requirement.

[120] 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 Gmail account, the transmission of the communication will be completed. If X is located within the British Islands at the time he logs into the Gmail 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.

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.

227. **Fourthly**, it is the safeguard in s. 16(2) RIPA that affords significant protections for persons within the British Islands at the stage of selection for examination, 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*"[121].

228. For all those reasons, any difference of view between the Applicants and Government as to the precise ambit of the definition of "external communications" in s.20 RIPA does not render the s.8(4) Regime contrary to Article 8(2) ECHR. The IPT was right so to conclude in the Liberty proceedings.

*The breadth of the concepts of "national security"/"serious crime"*

229. **First,** the ECtHR has consistently held in a long line of authority that the term "national security" is sufficiently foreseeable to constitute a proper ground for secret surveillance measures, provided that the ambit of the authorities' discretion is controlled by appropriate and sufficient safeguards. Most notably for present purposes, the applicant in *Kennedy* similarly asserted that the use of the term "national security" as a ground for the issue of a warrant under s.5(3) RIPA was insufficiently foreseeable; and that argument was rejected in terms by the ECtHR at §159.

230. Further, the Grand Chamber in *Zakharov* cited §159 of *Kennedy*; reiterated its observation that threats to national security may *"vary in character and be unanticipated or difficult to define in advance"*; and reasoned to the effect that a broad statutory ground for secret surveillance (such as national security) will not necessarily breach the "foreseeability" requirement, provided that sufficient safeguards against arbitrariness exist within the applicable scheme as a whole: see *Zakharov* at §§247-249 and 257[122]. In this case, for all the reasons already set out above such safeguards plainly exist, both by virtue of the detailed provisions of the Code, and by virtue of the oversight mechanisms of the Commissioner, the ISC and the IPT.

231. **Secondly**, the English Courts have not adopted a particularly unusual, surprising or broad

[121] For example, London-based person A undertakes a Google search. 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 (see Farr §134). 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.

[122] See too *Szabo* at §64 (where the Court stated that it was "not wholly persuaded" by a submission that a reference to "terrorist threats or rescue operations" was insufficiently foreseeable, "*recalling that the wording of many statutes is not absolutely precise, and that the need to avoid excessive rigidity and to keep pace with changing circumstances means that many laws are inevitably couched in terms which, to a greater or lesser extent, are vague."*

approach to the definition of "national security". The Applicants' submission to the contrary is wrong, and none of the cases upon which they rely supports their position[123] (*Secretary of State for the Home Department v Rehman* [2003] 1 AC 153, *R(Corner House) v Director of the Serious Fraud Office* [2009] 1 AC 756, *R v Gul* [2014] AC 1260 and *R(Miranda) v Home Secretary* [2014] 1 WLR 1340[124]). In *Rehman,* the House of Lords did no more than hold that national security was a "*protean concept*" which could be prejudiced by the promotion of terrorism in a foreign country by a UK resident, without any *"direct threat"* to the UK. That is unsurprising, and wholly consistent with the Court's own case law. The *Corner House, Gul* and *Miranda* cases did not address the meaning of "national security" at all, but rather the definition of "terrorism" in the Terrorism Act 2000. That is only a definition for the purposes of the Act: it does not purport to be a universal definition of "terrorism", still less of national security[125]. See §§6.81-6.90 of the Government's BBW Observations.

232. **Thirdly,** the s.8(4) Regime is designed so as to ensure that a person's communications cannot be examined by reference to unparticularised concerns of "national security". Rather, a specific and concrete justification must be given for each and every access to those communications; and the validity of that justification is subject to internal and external oversight. So the regime contains adequate safeguards against abuse by reference to an overbroad or nebulous approach to "national security". In particular:

(1) Communications cannot be examined at all unless it is necessary and proportionate to do so for one for one of the reasons set out in the certificate accompanying the warrant issued by the Secretary of State. Those reasons will be specific ones, which must broadly reflect the NSC's "Priorities for Intelligence Collection": see Code, §6.14. Moreover, the certificate is under the oversight of the Commissioner, who must review any changes to the descriptions of material within it: see Code, §6.14.
(2) Before communications are examined at all, a record must be created, setting out why access to the particular communications is required consistent with s.16 RIPA and the appropriate certificate, and why such access is proportionate: see Code, §7.16.
(3) The record must be retained, and is subject both to internal audit and to the oversight of the Commissioner (as well as that of the IPT). See Code, §7.18.

233. **Finally,** as to the contention that the meaning of "serious crime" in the s.8(4) Regime is insufficiently clear, at §159 of *Kennedy* the Court observed that RIPA itself contains a clear definition both of "serious crime", and what is meant by "detecting" serious crime: see s.81 RIPA.

234. In conclusion, for all the reasons set out above, the s.8(4) Regime is in accordance with the law for the purposes of Article 8 ECHR, and prescribed by law for the purposes of Article 10.

---

[123] See the BBW Application at §§106-110 and the Update Submissions at §§25-31

[124] *Rehman, Corner House* and *Miranda* are at Annexes 52, 53 and 54 respectively. *Miranda* is also at **CB/53**

[125] See s.1 Terrorism Act 2000, Annex 55.

**The s.22 Regime and foreseeability/accessibility**

235. The Government has explained at §§92-95 above why the s.22 Regime does not apply to the interception of communications data at all; why the BIJ Applicants cannot therefore conceivably claim to be victims of the regime; and why their complaint is brought on the basis of a fundamental misunderstanding. In light of that explanation, the specific complaints that they make about the s.22 Regime are addressed only briefly below, and only insofar as they differ from points already made above about the s.8(4) Regime. Their complaints are addressed in more detail at §§41-73 of the BIJ Further Observations of 16 December 2016.

236. The Applicants' fundamental complaint that there is no system for the *"independent authorisation of the interception of communications data"* under s.22 RIPA, and that this is contrary to the Article 8/10 rights of journalists and newsgathering organisations:

(1) This submission is premised on the misunderstanding that s.22 RIPA concerns the interception of communications data in the first place: see above.
(2) In any case, the submission is wrong even on its own terms. The Acquisition and Disclosure Code (in its most recent version from March 2015, **CB/32**) requires at §§3.78-3.84 that an application for communications data by a police force or a law enforcement agency which is designed to assist in the identification of a journalist's source should not be made be made under s.22 RIPA, but should instead be made under the Police and Criminal Evidence Act 1984, which requires judicial authorisation[126]. This is a complete answer to the BIJ Applicants' concern that the law enforcement authorities have previously used powers under s.22 RIPA to obtain disclosure of journalistic sources[127].
(3) The Applicants complain[128] that these provisions of the Acquisition and Disclosure Code only apply in cases where the identification of a journalistic source is "intended", and not in those cases where the "*identification of a source was not the intended purpose of the interception*". The short answer to this complaint, of course, is that the s.22 Regime is not concerned with interception, and there is nothing "unintentional" about its operation. If an application is made for an authorisation, it will by definition always be "intentional".
(4) Insofar as the Applicants are concerned that intercepted communications data could be used to obtain disclosure of journalists' sources, they ignore the provisions of the Code[129]. The Code provides at §§4.26-4.32 for the protection of confidential material, including

[126] There is an exception for cases where there is believed to be an immediate threat to human life, in which case the internal authorisation process of s.22 may be used, provided that such authorisations are notified to the Commissioner as soon as possible.
[127] See e.g. §97(c) of the BIJ Applicants' Obs in Reply.

[128] See §§115(c)-119 of their Obs in Reply.

[129] I.e. the Interception of Communications Code, rather than the Acquisition and Disclosure Code applying to Chapter 2 Part 1 RIPA.

journalistic material[130]. Such material should be retained only where it is necessary and proportionate for one or more of the authorised purposes in s.15(4) RIPA; must be securely destroyed when its retention is no longer needed for those purposes; and if it is retained, there must be adequate information management systems in place to ensure that retention remains necessary and proportionate. Where it is retained or disseminated to an outside body, reasonable steps should be taken to mark it as confidential, and where any doubt exists, legal advice should be sought before its dissemination. Further, any case where confidential material is retained should be notified to the Commissioner as soon as reasonably practicable, and the material concerned should be made available to the Commissioner on request.

**The s.8(4) Regime satisfies the "necessity" test**

237. As to the question whether the s.8(4) Regime is "necessary in a democratic society", the ECtHR has consistently recognised that when balancing the interests of a respondent State in protecting its national security through secret surveillance measures against the right to respect for private life, the national authorities enjoy a *"fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security"*: see e.g. *Weber* at §106, *Klass* at §49, *Leander* at §59, *Malone* at §81. Nevertheless, the Court must be satisfied that there are adequate and effective guarantees against abuse. That assessment depends on all the circumstances of the case, such as the nature, scope and duration of possible measures; the grounds required for ordering them; the authorities competent to authorise, carry out and supervise them; and the kind of remedy provided by the national law. See e.g. *Zakharov* at §232.

238. To the extent that the Applicants rely on *Szabo and Vissy* for the proposition that a different test of "strict necessity" is required, it is submitted that the test set out the Grand Chamber in *Zakharov,* and in a long line of other well-established cases, is to be preferred. It represents a properly protective set of principles which balance the possible seriousness of the Article 8 interference with the real benefits to the general community of such surveillance in protecting them against acts of terrorism and other national security threats. Strict necessity as a concept is used expressly in the Convention scheme where appropriate – indicating that it should not be imported elsewhere; or, if that is permissible at all, then only with the greatest caution. There is no warrant for any stricter test in principle in the present context.

239. However, whether viewed through the prism of general necessity, or adopting the test of "strict necessity" in the respects identified in *Szabo*, the s.8(4) Regime satisfies the necessity test.

240. The rationale for the s.8(4) Regime and its operation have been addressed on a number of occasions by independent bodies, viz. the IPT, the ISC, the Commissioner, the Anderson Report, and the Bulk Powers Review. Materially, the Anderson Report, the Bulk Powers Review and the ISC Report all conclude in terms, and with supporting analysis and detail, that less intrusive (or

[130] It is apparent from the drafting of Chapter 4 of the Code that references in the Chapter to "confidential journalistic material" are to the material intercepted under an interception warrant, including any related communications data, and that therefore those terms do not bear the technical meaning given to them in s.20 RIPA.

different) programmes could not address the legitimate needs of the UK. See above, §§14-31.

241. Although the Bulk Powers Review was not specifically tasked with opinion on whether bulk interception powers were proportionate, its conclusions are plainly highly material to that question, as summarised at §§27-29 above. At §§9.12-9.14 it stated:

> *"I have already summarised what I consider to be the strength of the operational case for each of the bulk powers (chapters 5-8 above). Among the other sources of evidence referred to in chapter 4 above, I have based my conclusions on the analysis of some 60 case studies, as well as on internal documents in which the SIAs offered frank and unvarnished assessments of the utility and limitations of the powers under review.*
>
> *The sheer vivid range of the case studies – ranging from the identification of dangerous terrorists to the protection of children from sexual abuse, the defence of companies from cyber-attack and hostage rescues in Afghanistan – demonstrates the remarkable variety of SIA activity. Having observed practical demonstrations, questioned a large number of analysts and checked what they said against contemporaneous intelligence reports, neither I nor others on the Review team was left in any doubt as to the important part played by the existing bulk powers in identifying, understanding and averting threats of a national security and/or serious criminal nature, whether in Great Britain, Northern Ireland or further afield.*
>
> *My specific conclusions, in short summary, are as follows:*
>
> *(a) The bulk interception power is of vital utility across the range of GCHQ's operational areas, including counter-terrorism, cyber-defence, child sexual exploitation, organised crime and the support of military operations. The Review team was satisfied that it has played an important part in the prevention of bomb attacks, the rescuing of hostages and the thwarting of numerous cyber-attacks. Both the major processes described at 2.19 above [i.e. the "strong selector" and "complex query" process] produce valuable results. Communications data is used more frequently, but the collection and analysis of content has produced extremely high-value intelligence, sometimes in crucial situations. Just under 50% of GCHQ's intelligence reporting is based on data obtained under bulk interception warrants, rising to over 50% in the field of counter-terrorism."* (emphasis added)

242. In light of the facts set out at §§14-31 above, to describe the Government's bulk interception as "*a speculative fishing exercise, designed to check the behaviour of an entire population*" (see §212 of 10 HR Obs in Reply) could not be further from the truth. It is a capability which is of "*vital utility*" in identifying and averting threats of a national security and/or serious criminal nature.

243. Thus, this part of the Applicants' submissions both factually mischaracterises the operation of the s.8(4) Regime; and ignores the vital point that the interception of a bearer's entire contents is the only way for the Intelligence Services to obtain the external communications they need to examine for national security purposes. They need the "haystack" to find the "needle"; and the "haystack" is itself carefully selected. Communications are not intercepted on the basis of "happenstance" (or to put it another way, simply because they can be). The s.8(4) Regime operates on the basis that the Intelligence Services will identify the particular bearers that are most likely to carry "external communications" meeting the descriptions of material certified by the Secretary of State, and will intercept only those bearers. See the Code, §6.7. Moreover, and as the Code also states:

(1) The Intelligence Services must conduct the interception in ways that limit the collection of non-external communications to the minimum level compatible with the object of intercepting wanted external communications (Code, §6.7);
(2) The Intelligence Services must conduct regular surveys of relevant bearers, to ensure that they are those most likely to be carrying the external communications they need (Code, §6.7);
(3) Any application for a warrant authorising the interception of a particular bearer must explain why interception of that link is necessary and proportionate for one or more of the purposes in s.5(3) RIPA (Code, §6.10);
(4) If an application is made for the warrant's renewal, the application must not only state why interception of the bearer continues to be proportionate, but must also give an assessment of the intelligence value of material obtained from the bearer to date (Code, §6.22).

244. If the Intelligence Services were unlawfully intercepting bearers on the basis of "happenstance", that is something that would be picked up by the Commissioner as part of his survey of warrants and their justification. But the Commissioner has found the opposite: see e.g. his investigation of the s.8(4) Regime in the 2013 Report at §6.5.42 (Annex 11, **CB/35**).

245. If the Applicants wish to say that intercepting the contents of a bearer is inherently disproportionate, they must accept as a corollary the real possibility that the Intelligence Services will fail to discover major threats to the UK (such as a terrorist bomb plot, or a plot involving a passenger jet – see e.g. examples 2 and 6 in Annex 9 to the Anderson Report[131]). It would be absurd if the case law of the ECtHR required a finding of disproportionality in such circumstances, merely because the whole contents of a communications link are intercepted, even though only a tiny fraction[132] of intercepted communications are ever, and can ever be, selected for potential examination, let alone examined. On a proper analysis, it does not. See/compare *Weber* and §145 above.

246. As to the Applicants' reliance on cases involving the bulk *retention* of data (see e.g. §§203, 207-209 of the 10 HR Applicants' Obs in Reply), those are irrelevant to the issues raised in these Applications, which involve bulk interception followed by targeted selection of material. This is not a situation where there is bulk retention of data on an "indiscriminate" basis[133].

247. Finally, the bulk interception process involves the discarding of unwanted communications and does not permit "*the storing and analysing of collateral data*" (*contra* the 10HR Applicants' Obs in Reply at §213). That was made clear in the Bulk Powers Review at §§2.16 and 2.17. The second (filtering) stage involves discarding those bearers least likely to be of intelligence value and the third (selection) stage involves automatically discarding all communications that do not match the chosen selection criteria.

[131] See Annex 14, **CB/48**

[132] I.e. on the basis that it is necessary and proportionate to do so, because they are of legitimate intelligence interest.

[133] See §§207-208 of the 10 HR Applicants' Obs in Reply

**Question 4: If the Applicants brought proceedings before the IPT, did those proceedings involve the determination of "civil rights and obligations" within the meaning of Article 6(1) of the Convention?**

248. The answer to this question is "no". The Court/Commission have consistently held that decisions authorising surveillance do not involve the determination of "civil rights and obligations" within the meaning of Article 6(1). In particular:

(1) In *Klass*, the Commission (Report of the Commission, Series B, no. 26 pp. 35-37) concluded that the applicants' right to protection of secrecy for correspondence and telecommunications was not a "civil" right for the purposes of Art. 6(1), because surveillance of this kind involved the exercise of State authority in the public interest, which did not concern private rights of the kind covered by Article 6. See §58:

> *"...to determine what is the scope meant by 'civil rights' in Art. 6, some account must be taken of the legal tradition of the Member-States. Supervisory measures of the kind in question are typical acts of State authority in the public interest and are carried out jure imperii. They cannot be questioned before any court in many legal systems. They do not at all directly concern private rights. The Commission concludes therefore, that Art. 6 does not apply to this kind of State interference on security grounds."*

(2) The Court in *Klass* found it unnecessary to reach a conclusion on whether Art.6 ECHR applied after the applicant had been notified of surveillance, on the basis that he had in any event sufficient legal remedies at that point: but it too held that prior to such notification, Article 6 could not apply. See §75[134].

(3) The Court has since approved the Commission's approach in *Klass.* See *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* app. 62540/00, 28 June 2007, at §106: a case which concerned the compatibility of Bulgarian legislation allowing the use of secret surveillance measures with Articles 6, 8 and 13 ECHR. It may be noted that the IPT's own finding to the contrary in the domestic proceedings which resulted in *Kennedy v UK* was reached before the *Ekimdzhiev* case was decided (and the Court in *Kennedy* did not endorse the IPT's conclusion, though it concluded that in any event Article 6 had not been breached[135].)

---

[134] *"As long as it remains validly secret, the decision placing someone under surveillance is thereby incapable of judicial control on the initiative of the person concerned, within the meaning of Article 6; as a consequence, it of necessity escapes the requirements of that Article."*
The Court's approach to Art. 6 in *Klass* is consistent with the approach to Art. 13 in the context of secret surveillance powers – see eg. *Leander v Sweden* at §77(d).

[135] For that reason, the 10 HR Applicants are plainly wrong to rely on *Kennedy* as authority that Article 6 applies: it is not. See/compare §§273-274 of the 10HR Obs in Reply.

249. The Court's conclusion in *Ekimdzhiev* that the rights at issue in the field of secret interception powers are not "civil" rights is supported by the Court's more general jurisprudence on the meaning of "civil rights and obligations". The Grand Chamber in *Ferrazzini v Italy* app. 44759/98, 12 July 2001 has indicated that the exercise of powers forming part of the "*hard core of public-authority prerogatives*" of the State will not amount to "civil rights and obligations" for the purposes of Article 6(1): see *Ferrazzini* at §§27-29[136] (and see also the similar reference to "discretionary powers intrinsic to state sovereignty" at §61 of *Vilho Eskelinen v Finland*, app. 63235/00, 19 April 2007). Secret powers of intelligence gathering/interception that are used solely in the interests of national security or to detect serious crime are quintessentially part of that "hard core of public authority prerogative".

250. As the Grand Chamber confirmed at §38 of *Maaouia v France*, app. 39652/98, 5 October 2000, the fact that a dispute may have major repercussions for an individual's private life does not suffice to bring proceedings within the scope of "civil" rights protected by Art. 6(1).

251. Nor does the fact that the Applicants had the right, as a matter of domestic law, to complain to the IPT make the rights at issue "civil". As recognised by the Grand Chamber in *Ferrazzini* at §24, the concept of "civil rights and obligations" is "autonomous" within the meaning of Art. 6(1). Thus, it cannot be interpreted solely by reference to the domestic law of the respondent State. So the mere fact that the IPT offered the 10 HR applicants recourse to test the lawfulness of any surveillance that might have occurred does not make any difference to the Article 6 analysis (*contra* §§276-279 of the 10 HR Obs in Reply).

252. Finally, and for good measure, the IPT is specifically designed to operate under the constraints recognised by the Court at §57 of *Klass* (and upon which the Court's conclusion at §75 of *Klass* that Article 6 could not apply before an applicant had been notified of surveillance was based). A complainant in the Tribunal is not permitted to participate in any factual inquiry that the Tribunal may conduct into the allegations that he has made, and the fact of any interception remains secret throughout (unless the Tribunal finds at the <u>end</u> of the proceedings that unlawfulness has occurred). The Liberty proceedings involving the 10 HR applicants were no different in this respect. The Government neither confirmed nor denied that interception had occurred, and the parties' arguments in the case proceeded on assumed facts. So the reasoning of the Court in *Klass* applies here too (quite apart from the general, and determinative, point made above concerning the exercise of the *"hard core of public authority prerogative"*).

**<u>Question 5: If Article 6 applied, were the limitations in the IPT proceedings, taken as a whole, disproportionate or did they impair the very essence of the Applicants' right to a fair trial?</u>**

[136] The Court stated that procedures classified under national law as part of "public law" could come under the civil head of Article 6 if their outcome was decisive for private rights such as e.g. the sale of land, or the grant of a licence; but that rights and obligations for an individual are not necessarily "civil" in nature, and this will be the case where, as is the case with tax obligations, they form "*part of the hard core of public authority prerogatives, with the public nature of the relationship between the taxpayer and the community remaining predominant…"*

253. The answer to this question is "no". Even if Article 6 had applied to the proceedings before the IPT, it would have been satisfied. The IPT's procedures, which must take account of the legitimate need to protect sensitive information, plainly did not impair the very essence of the Applicants' right to a fair trial, particularly given the Court's reasoning and conclusions in *Kennedy.*

***The relevant principles***

254. The Court will not find a violation of the right to a fair trial unless satisfied that the applicant has been deprived overall of that right (i.e. it considers proceedings as a whole); and the constituent elements of a fair trial are not rigid and uniform, but dependent upon the context and circumstances. See e.g. *Dombo Beheer v The Netherlands* app. 14448/88, 27 October 1993, *CG v United Kingdom* app. 43373/98, 19 December 2001. The requirements inherent in the concept of a fair hearing are not necessarily the same in civil as in criminal cases: the contracting States have greater latitude when dealing with civil cases than with criminal: see e.g. *Vanjak v Croatia* app. 299889/04, 14 January 2010 at §45.

255. As to **disclosure,** the Court's clear and consistent jurisprudence recognises that the protection of national security interests provides a legitimate basis on which material can be withheld. The Court assesses whether a particular limitation is permissible by reference to two factors: (1) to be "strictly necessary" the restriction must be directed to a proper social objective and go no further than required to meet that objective; and (2) the restriction must be "sufficiently counterbalanced" by the procedures allowed by the judicial authorities so as not to impair the "very essence of the right": see e.g. *Tinnelly & Sons Ltd v UK* app. 20390/92, 10 July 1998, §72; *Rowe and Davis v UK* app. 28901/95, 16 February 2000 (GC), §61; *Leander v Sweden* §§49, 59, 63; *Kennedy* §§180, 184–190. When making that assessment, the extent of disclosure required may depend upon the nature of the rights at issue. The right to liberty, for example, may justify more extensive disclosure obligations than the right to challenge secret vetting: see/compare *Leander, Esbester v UK* and *Kennedy.*

256. Most materially for present purposes, the Court specifically considered the nature of the processes applied by the IPT in this context in detail in *Kennedy,* and concluded that the restrictions on disclosure, and on the provision of reasons, applied through the IPT Rules did not impair the essence of the right to a fair trial. (Indeed, in the Government's submission, they enhanced it, by making it possible for the IPT to deal with the issues on the basis of as full as possible an understanding of the facts and background[137]). See §§186-190 of *Kennedy*.

***Application to the facts***

257. In the Government's submission, all the same points made in *Kennedy* equally explain why the 10 HR Applicants in this case had a fair hearing in domestic proceedings:

[137] See/compare the remarks of Lord Brown in *R(A) v Director of Establishments of Security Service* [2010] 2 AC 1 at §14, cited at §63 above

(1) The applicants did not have to overcome any evidential burden to apply to the IPT;
(2) There was scrutiny of all the relevant material, open and closed, by the IPT, which had full powers to obtain any material it considered necessary;
(3) Material was only withheld in circumstances where the IPT was satisfied that there were appropriate public interest and national security reasons for doing so;
(4) The Tribunal appointed CTT who, in practice, performed a similar function to that performed by a Special Advocate in closed material proceedings. CTT was well placed to represent the interests of the Applicants in closed hearings given the issues which the IPT was considering (which did not turn on specific instructions from the Applicants themselves).

258. **First** it is said by the 10 HR Applicants that the IPT declined to direct the intelligence services to disclose any of their internal guidance concerning the treatment of confidential material of non-government organisations (NGOs) under Art. 10[138]. This is addressed at §§134-135 of the IPT's 5 December Judgment. As is evident from that extract, the Applicants only sought to raise the issue of "NGO Confidence" at a very late stage of the IPT proceedings (in written submissions dated 17 November 2014, several months after the open hearing of July 2014 to deal with disputed legal issues, and many months after the parties agreed the legal issues for the hearing (February 2014)). The IPT concluded that it was far too late to raise the issue, particularly where it was suggested that further disclosure and considerable further argument would be necessary to incorporate it into the proceedings at that stage. The IPT cannot possibly be criticised for this approach. It followed that no question of disclosure on this issue arose in the first place. In any event, disclosure generally was not a live issue in the hearing, in circumstances where the Intelligence Services agreed voluntarily to make all of the disclosure which the IPT held should be made, consistent with national security. See §10 of the IPT's 5 December Judgment.

259. **Secondly,** the Applicants assert that the IPT wrongly held a closed hearing on "in accordance with the law" issues. There was no breach of Art. 6 in that approach. As explained by the IPT, the matters which were considered in closed were too sensitive for discussion in open court for reasons of national security. In addition, part of the purpose of considering the agencies' internal arrangements in closed was to consider their adequacy and whether any of them could be publicly disclosed – see §7 and 46(iii)-(iv) of the 5 December judgment. Further, CTT was appointed, and made submissions from the perspective of the Applicants, both on the issue of disclosure and in order to ensure that all relevant arguments on the facts and law were put to the IPT.

260. **Thirdly,** it is said in the 10 HR Observations that the IPT refused to hear and decide one of the preliminary issues that was agreed between the parties, namely whether the respondents' NCND policy in relation to the existence of particular interception programmes was justified. However, as is evident from §13 of 5 December Judgment, that issue was not decided by the IPT

[138] See 10 HR Observations, §76.

by agreement between the parties[139].

261. 10 HR make certain other complaints about the IPT in their "Submissions made in Light of the third IPT Judgment" and Obs in Reply. Those equally have no basis. Addressing them briefly:

(1) The complaint that the IPT failed to assess the general proportionality of the s.8(4) Regime[140] is wrong: see §48 above. The IPT expressly dealt with the issue, and both parties made full disclosure on it (insofar as open disclosure was possible) prior to the *inter partes* open hearing.

(2) It is said that determinations in favour of Amnesty International and the Legal Resource Centre show that the Intelligence Services "deliberately targeted" the communications of human rights organisations[141]. In fact, they show the opposite. See §§49-51 above.

(3) The Applicants complain that they are unable to understand how the IPT reached the conclusion that there had been lawful and proportionate interception and accessing in the two individual cases (see §§26-30 of their submissions on the Third Judgment). But that is a function of the fact that the IPT is required by Rule 6(1) to ensure that information is not disclosed to an extent or in a manner which would be contrary to the public interest or prejudicial to national security. That was emphasised by the IPT at §13 of its 22 June 2015 judgment, where it made clear that the IPT could only provide the essential elements of its determination, because to do otherwise would offend against that important rule.

(4) The Applicants assert that there was a failure to address Art. 10 ECHR in the 22 June judgment. But the Applicants do not make clear what Art. 10 would have added to the IPT's consideration of the individual cases or the IPT's conclusion that it was lawful and proportionate to intercept/access the material. These submissions appear to be premised on the basis that it would have been unlawful for the Intelligence Agencies to have deliberately targeted the e-mails of human rights organisations and that such deliberate targeting would have been disproportionate under Art. 10 ECHR. But that is not a proper inference which can be drawn from the terms of the 22 June 2015 judgment for the reasons set out above.

(5) The Applicants criticise the IPT for failing to make clear whether the "accessing" of Amnesty's/LRC's communications involved their communications data. This criticism is wholly misplaced. Had the IPT considered that any communications data pertaining to Amnesty, the Legal Resource Centre, or any other applicant, had been handled unlawfully, it

---

[139] §13 of the judgment states: *"There were also certain of the Agreed Issues (Issue xii), (xiii) and (xiv) which were described as "Issues of law relating to procedure", and which, by agreement, have not fallen for decision at this hearing. They relate in part to the NCND policy, the importance of which is emphasised by the Respondents in the following paragraphs of their Open Response…* (emphasis added)
In any event, the Court has itself recognised the importance of the "neither confirm nor deny" approach in maintaining the efficacy of a secret surveillance system, see e.g. *Klass* at §58, *Weber* at §135. Significantly in *Kennedy* at §187 the Court accepted that the governments' NCND policy was a valid basis on which eg. documents submitted to the IPT would be highly sensitive and therefore incapable of being disclosed.

[140] Additional Submissions, §§16-17.

[141] Additional Submissions, §§18-25.

would have said so in its judgment.

262. **Finally**, the Applicants have impugned the IPT's independence, on the basis that it held a meeting with the Security Service in 2007 as part of its work. That is a meritless suggestion. The IPT is a specialist tribunal, and the nature of its casework means it is necessary for its members to have a level of background understanding regarding the Intelligence Services' practices and procedures. The meeting which occurred on 28 September 2007 (as recorded in a Note for File dated 15 November 2007, **CB/11**) was an entirely appropriate example of that. Its purpose was simply a "general briefing", including about the Security Service's data handling techniques, and it occurred around 6 years before these claims were brought. It cannot sensibly be said that this undermines the IPT's independence: see §56 of the Government's 10HR Further Submissions of 16 December 2016.

**Question 6: Has there been a breach of Article 14, taken together with Art 8/10, on account of the fact that section 16 RIPA grants additional safeguards to people known to be in the British Islands?**

263. The Applicants contend that the s.8(4) Regime is indirectly discriminatory on grounds of nationality contrary to Article 14 ECHR, because persons outside the United Kingdom are *"disproportionately likely to have their private communications intercepted"*[142] and/or because s.16 RIPA grants *"additional safeguards to persons known to be in the British Islands";* and, it is said, that difference in treatment is not justified. The true position is as follows:

(1) The operation of the s.8(4) Regime does not mean that persons outside the UK are disproportionately likely to have their private communications intercepted.
(2) At the stage when communications are selected for examination, the s.8(4) Regime provides an additional safeguard for persons known to be within the British Islands.
(3) However, the application of that safeguard to persons known to be within the British Islands, and not to persons outwith the British Islands, does not constitute a relevant difference in treatment for the purposes of Article 14 ECHR.
(4) Moreover, even if it did constitute a relevant difference in treatment for the purposes of Article 14, it would plainly be justified.

*What is the relevant difference in treatment, if any?*

264. "*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 outside the British Islands are therefore not necessarily any more likely than persons within the British Islands to have their communications intercepted under a regime which focuses upon certain types of "*external communication*"; particularly if, as is alleged, the regime operates in relation to fibre optic cables within the British Islands. The sole respect in which persons may be treated differently by reason of current location under the s. 8(4) Regime

[142] See the Applicants' Additional Submissions, §83.

is that at the selection stage, limitations are imposed on the extent to which intercepted material can be selected according to a factor referable to an individual known to be for the time being in the British Islands (for example, a UK landline telephone number). Before such a course may be taken, the Secretary of State must certify that it is necessary under s.16 RIPA.

265. However, the ECtHR's case law has indicated that mere geographical location at any given time is not a relevant difference in status for the purposes of Article 14: see *Magee v United Kingdom* app. No. 28135/95, ECtHR, 6 June 2000, at §50. (The Applicants' reliance on *Carson v United Kingdom* App. No. 42184/05, 16 March 2010 is misplaced: *Carson* concerns residence, which is a relevant difference, but residence has a degree of permanency that mere location does not.)

*Justification*

266. 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 the State to show that the difference in treatment has a rational justification and is not "manifestly without reasonable foundation": see e.g. *Stec v United Kingdom* app. 65731/01, Grand Chamber, 12 April 2006 at §52. The margin of appreciation is also commensurately greater, where questions of national security are concerned (see *Weber* at §106, *Klass* at §49, *Leander* at §59, *Malone* at §81). Thus, to the extent that Art 14 is engaged at all, the present circumstances are ones in which the Government is to be afforded a wide margin of appreciation. It need show only that the differential treatment at issue is not manifestly without reasonable foundation. There is plainly a rational justification for treating persons known to be in the British Islands, and persons not known to be in the British Islands, differently under s. 16 of RIPA, as the IPT rightly found in the Liberty proceedings.

267. The Government has considerable powers and resources to investigate a person within the British Islands, without any need to intercept their communications under a s. 8(4) warrant. See Farr §§145-146, Annex 3. For instance, the Security Service can search their details against open source information; make enquiries with a local police force; deploy surveillance against the person's address; and apply to major telephone and internet service providers for a "*subscriber check*" to determine the name of any subscriber for telephone and broadband services at that address. Once a broadband line has been identified, that specific line can be intercepted. All these factors explain why it should generally be feasible to intercept the communications of a person within the British Islands through a warrant under s.8(1) RIPA naming that person, or their property, and setting out in a schedule the factors to be used to identify the communications to be intercepted.

268. That being so, the circumstances in which it is necessary to attempt to obtain the communications of a person in the British Islands under a s. 8(4) warrant should be relatively rare. So it is practicable and proportionate for the Secretary of State to consider each such instance, and (if appropriate) certify that this is indeed necessary under s. 16(3) RIPA:

(1) As a matter of proportionality, it is important to consider whether the communications could be obtained by other, more specifically targeted, means; and
(2) Selection of material obtained under a s. 8(4) warrant should not be used as a means of evading the type of controls in s. 8(1) of RIPA.

269. Conversely, the Government will not usually have anything like the same powers to investigate a person outside the British Islands, without the use of a s. 8(4) warrant. So the circumstances in which the Government will need to examine material obtained under a s. 8(4) warrant for the purpose of obtaining the communications of specific individuals outside the British Islands are commensurately wider. That is sufficient justification for treating the two cases differently.

270. The Applicants nevertheless assert that differential treatment cannot be justified, because GCHQ is able to exercise an "*identical degree of control*" over all communications passing through fibre optic cables that they intercept, whether they be between Birmingham and London, or Toronto and Cairo: Additional Submissions, §84. That analysis is wrong for a number of reasons (upon which, contrary to 10 HR's Obs in Reply[143], the Government gave evidence to the IPT both in open and closed – see for the open evidence e.g. Farr §§143-147):

(1) It ignores the fact that the Government has a panoply of powers to investigate a person in Birmingham, which it does not have to investigate a person in Baghdad. In general, the Government should able to investigate an identifiable Birmingham-based individual without the need for a s. 8(4) warrant at all; not so for the individual in Baghdad.
(2) It assumes that the Intelligence Services are likely to have the same base of knowledge from which to identify the communications of a person in Baghdad, as they would have for a person in Birmingham. That assumption is wholly unjustified. Because the Government does not have the same powers to investigate individuals outside the British Islands, it may not know exactly who the individual in Baghdad is; or may have an online identity for him, without a name; or may have a variety of aliases, without knowing his true identity. Yet the logic of the Applicants' position is that in all such cases, the use of any combination of factors to identify that individual's communications would have to be certified by the Secretary of State, because any such factors would be "referable" to him.
(3) It ignores the fact that the number of cases in which it is necessary to identify the communications of individuals in the British Islands using a s. 8(4) warrant are relatively rare by comparison with the communications of individuals outside the British Islands, for all the reasons set out above. So the questions of practicality that would arise, were it necessary for the Secretary of State to certify all factors relating to such individuals, are commensurately much more acute.

271. Put another way, on the Applicants' case, if one were interested in the communications from or to (say) a thousand British Jihadists in Syria and Northern Iraq, use of any factor or combination

[143] See the 10 HR Obs in Reply, §271(4)

of factors that was designed to elicit communications from or to any individual Jihadist would require consideration by, and consequent certification from, the Secretary of State. Whether or not that would make the entire selection process unworkable, it indicates at the very least why there is a rational justification for treating persons *"for the time being in the British Islands"* differently under s. 16(2), from persons not in the British Islands.

## IV. CONCLUSION

272. In these circumstances, the Government invites the Court to declare these applications inadmissible on the specific grounds set out above and/or as manifestly ill-founded; alternatively to decide on the merits that there has been no violation of the Convention.

Verity Robson

Verity Robson

29 September 2017 (Agent of the Government of the United Kingdom)

**Glossary**

| | |
|---|---|
| The 10 HR Applicants | The 10 Human Rights Organisations bringing application number 24960/15 |
| The Acquisition and Disclosure Code | The Code of Practice for the Acquisition and Disclosure of Communications Data, last updated in May 2015, issued under s.71 RIPA. This addresses (inter alia) the acquisition of data under Chapter 2 of Part 1 RIPA |
| The Anderson Report | A report of June 2015 by the Investigatory Powers Review, conducted by David Anderson QC, entitled "A Question of Trust" |
| The BBW Applicants | Big Brother Watch, Open Rights Group, English Pen and Dr Constanze Kurz |
| The BIJ Applicants | The Bureau of Investigative Journalism and Alice Ross |
| 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 Bulk Powers Review | A report of August 2016 by the Independent Reviewer of Terrorism Legislation (David Anderson QC), entitled "Report of the Bulk Powers Review". |
| The CJEU | Court of Justice of the European Union |
| The Code | The current Interception of Communications Code of Practice, issued on 15 January 2016 under s. 71 of RIPA |
| The 2002 Code | The previous version of the Interception of Communications Code of Practice, issued in July 2002 |
| The Commissioner | The Interception of Communications Commissioner, appointed under s. 57(1) RIPA. The Commissioner's functions have been taken over by the Investigatory Powers Commissioner from 1 September 2017. |
| 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 |
| CSP | Communications Service Provider |

| | |
|---|---|
| The CTA | The Counter-Terrorism Act 2008 |
| The DPA | The Data Protection Act 1998 |
| The Disclosure | The disclosure of certain internal safeguards within the Intelligence Sharing and Handling and s.8(4) regimes, given by the respondents in the Liberty proceedings, and recorded by the IPT in its 5 December and 6 February Judgments. |
| DRIPA | Data Retention and Investigatory Powers Act 2014 |
| External communication | A communication "sent or received outside the British islands" (see s. 20 of RIPA, and §6.1 of the Code) |
| FISA | The USA's Foreign Intelligence Surveillance Act 1978 |
| FISC | Foreign Intelligence Surveillance Court, charged with overseeing activities of the US intelligence agencies under FISA |
| 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 Regime | The regime (set out in "Domestic Law and Practice") 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, in the context of the allegations made by the Applicants (i.e. allegations about the receipt of intelligence from the Prism and Upstream programmes) |
| 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 |
| The IPT | The Investigatory Powers Tribunal |
| The IPT Rules | The Investigatory Powers Tribunal Rules 2000, SI 2000/2665 |
| The ISA | The Intelligence Services Act 1994 |

| | |
|---|---|
| The ISC | The Intelligence and Security Committee of Parliament |
| The ISC Report | A report of 17 March 2015 by the ISC, "Privacy and Security: a Modern and Transparent Legal Framework" |
| The ISC's Statement of 17 July 2013 | A statement made by the ISC following an investigation into the arrangements GCHQ has with its overseas counterparts for sharing intelligence, in light of allegations in the media that GCHQ had circumvented UK law by accessing information obtained by the NSA via Prism. |
| The JSA | The Justice and Security Act 2013 |
| The Liberty proceedings | Proceedings in the IPT brought in 2013 by Liberty, Privacy, Amnesty International and various other civil liberties organisations, challenging the Intelligence Sharing and s.8(4) Regimes, in the same factual premises as are relevant to the present application |
| The NSA | The National Security Agency |
| The NSC | The National Security Council |
| The OSA | The Official Secrets Act 1989 |
| PCLOB | Privacy and Civil Liberties Oversight Board, an independent bipartisan agency within the US government's executive branch, charged with ensuring that the federal government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties |
| PCLOB's 2 July Report | A report of 2 July 2014 of PCLOB, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act" |
| The Privacy 2 Judgment | A judgment of the IPT dated 8 September 2017, concerning powers of GCHQ to obtain and handle bulk data |
| RIPA | The Regulation of Investigatory Powers Act 2000 |
| 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 "Domestic Law and Practice" in the Government's Observations in the respective applications) that governs the interception of external communications and the handling and use of the intercepted material and communications data obtained as a result |
| A s. 8(4) warrant | An interception warrant issued under the s. 8(4) regime that complies with ss. 8(4)-(6) of RIPA |
| The s.16 arrangements | the safeguards applying under s.16 RIPA to the examination of intercepted material gathered under a s. 8(4) warrant |
| The s.22 Regime | The statutory regime (set out in the Government's Further Observations of 16 December 2016 in the BIJ application) governing the acquisition of communications data from communications service providers under s.22 RIPA |
| The Section 215 Programme | A US programme, conducted under the authority of s.215 of the US Patriot Act, involving the collection of telephone metadata in bulk, terminated in November 2015. The programme was unconnected with Prism and Upstream, and was conducted under different legal authority |
| SIS | The Secret Intelligence Service |
| The SSA | The Security Service Act 1989 |