Application No. 58170/13

IN THE EUROPEAN COURT OF HUMAN RIGHTS

BETWEEN:

10 HUMAN RIGHTS ORGANISATIONS

Applicants

-and-

THE UNITED KINGDOM

Respondent

THE UNITED KINGDOM'S OBSERVATIONS ON THE MERITS

Glossary

The Anderson Report	*A report of June 2015 by the Investigatory Powers Review, conducted by David Anderson QC, entitled "A Question of Trust"*
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) (See **Annex 59**)*
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; currently Sir Stanley Burnton*
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*
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*
Internal communication	*A communication that is not an external communication*
The IPT	*The Investigatory Powers Tribunal*
The IPT's 5 December Judgment	*The judgment of the IPT of 5 December 2014 in the Liberty proceedings*
The IPT's 6 February Judgment	*The judgment of the IPT of 6 February 2015 in the Liberty proceedings*
The IPT's 22 June Judgment	*The judgment of the IPT of 22 June 2015 in the Liberty proceedings*
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 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*

RIPA	*The Regulation of Investigatory Powers Act 2000*
The Rules	*The Investigatory Powers Tribunal Rules 2000, SI 2000/2665*
A s. 8(1) warrant	*An interception warrant that complies with s. 8(2)-(3) of RIPA*
The s. 8(4) Regime	*The statutory regime (set out in "Domestic Law and Practice") 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*
SIS	*The Secret Intelligence Service*
The SSA	*The Security Service Act 1989*

Contents ***Pages***

INTRODUCTION AND EXECUTIVE SUMMARY

1. This Application challenges the United Kingdom's legal regimes governing (i) the receipt of intercept material from the US authorities under the US Government's "Prism" and "Upstream" programmes (the "Intelligence Sharing Regime"); and (ii) the "bulk" interception of communications under s.8(4) of the Regulation of Investigatory Powers Act ("RIPA") (See Annex 1), pursuant to the alleged "Tempora" interception operation ("the s.8(4) Regime"). The detail of the answers given by the Government to these challenges is set out in the body of the Observations below. The level of detail required has inevitably lengthened the Observations. Accordingly, this Executive Summary indicates both the structure of the Observations and provides a summary of the key points made in them given.

2. This is an application of the utmost importance to the UK. It is 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 both the Intelligence Sharing Regime and the s.8(4) Regime have been and remain critical to the proper protection of national security, notably against the serious threat from terrorism. Recent events across Europe, including the recent terrorist attacks in Paris and Brussels, and a number of thwarted terrorist plots[1], have emphasised in the clearest way the nature of that threat and its devastating consequences, including the taking of innocent lives. Under the Convention scheme, it is properly for States to judge what systems are necessary for the protection of the general community from such threats.

3. It is of course acknowledged that the Convention scheme subjects those systems to ultimate European supervision. It does so because there are privacy interests in play. They are to be weighed against the need for the State to fulfil its paradigm, protective responsibility. The core purpose and fundamental aim of the Court's Article 8 jurisprudence has been and remains to ensure that the systems, operating as they must in secret, provide appropriate protection against abuse and arbitrariness by the

[1] For example, the plot to send suicide bombers onto 7 trains in Munich over Christmas 2015.

State. It is important that, in assessing the detail of appropriate protection, care is taken not to risk undermining the proper effectiveness of the systems for obtaining life-saving information and intelligence that cannot be obtained any other way. That is why the Court has consistently and rightly afforded States a broad margin of appreciation in determining whether measures that interfere with privacy are justified in the field of national security.

4. Some assert that the growth in the volume of internet traffic, and developments in technology, must necessitate a new legal approach or more safeguards. For example, it is suggested that no interception of any communications be undertaken at all, without reasonable suspicion in respect of the particular communication intercepted: an approach which would in practice (for reasons set out below) completely nullify the UK's ability to obtain intercept material from communications bearers. However, the scale of potential collection at the time that the Court previously considered bulk interception regimes in *Weber and Saravia v Germany*, app. 54934/00, ECHR 2006-XI ("*Weber*") and *Liberty v UK* app. 58243/00, 1 July 2008 ("*Liberty*") was already very considerable. Equally, traditional collection of traffic from communications satellites (undertaken by nearly every State) has inevitably always involved the interception of communications bearers carrying many hundreds of thousands if not millions of communications bundled together. There is no essential difference of kind between the UK's surveillance of communications obtained through interception of communications bearers, and the "strategic monitoring" addressed in *Weber*. The legal framework applied by the Court in *Weber* and *Liberty* has proved itself entirely adequate to control the use of interception by Council of Europe States.

5. By contrast, what has certainly changed is 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.

6. 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 detail is set out below (in **Section 2**). The bedrock of these Regimes are 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 Intelligence and Security Committee, "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 (see **§§1.19-1.35, §§2.26-2.41, §§2.105-2.124**). So too has the independent person appointed to keep terrorism laws under review, David Anderson QC. His report also contains useful material in the context of the present issues (see **§§1.21-1.35**).

7. The IPT is of particular importance in this case. That is because it conducted a conspicuously thorough and detailed examination of the very same issues that the Applicants now raise in the Liberty proceedings.[2] (see **§§1.41-1.51**) 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. It 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 context, there were some relevant aspects (both relating to

[2] 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.

the facts relating to the Applicants and relating to the nature of the safeguarding Regimes) 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 assisted 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[3].

8. In the Observations below, the Government begin by setting out some important points to be noted on the facts; and then the relevant domestic law and practice. The Government then addresses the questions posed by the Court in the following order below:

(1) ***Question 1:*** Whether in relation to the Intelligence Sharing Regime: (a) the Applicants can claim to be victims of violations of their rights under Article 8 ECHR; and (b) the acts of the UK are "in accordance with the law" and necessary within the meaning of Article 8 (**§§3.1-3.41**).

(2) ***Question 2:*** Whether in relation to the s.8(4) Regime: (a) the Applicants can claim to be victims of violations of their rights under Article 8 ECHR; and (b) the acts of the UK are "in accordance with the law" and necessary within the meaning of Article 8 (**§§4.1-4.108**).

(3) ***Question 3:*** The impact of the Applicants' status as NGOs on the Article 8 analysis (**§§5.1-5.4**).

(4) ***Question 4:*** Whether in relation to the s.8(4) Regime the acts of the United Kingdom are "prescribed by law" and necessary in a democratic society within the meaning of Article 10 ECHR (**§§6.1-6.39**).

(5) ***Question 5:*** Whether the proceedings before the IPT involved the determination of "civil rights and obligations" within the meaning of Art. 6(1). If so, whether the restrictions in the IPT proceedings taken as a whole were disproportionate or impaired the very essence of the applicants' right to

[3] 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.

a fair trial (**§§7.1-7.50**).

(6) ***Question 6:*** Whether there has been a violation of Article 14 taken together with Article 8 and/or Article 10 on account of the fact that the safeguards set out in s.16 of RIPA 2000 grants additional safeguards to people known to be in the British Islands? (**§§8.1-8.16**)

The facts and domestic law and practice

9. The Applicants' factual case both on the Intelligence Sharing and s.8(4) Regimes mischaracterises the nature of activities carried out under both regimes. In so doing, it reflects important misunderstandings perpetuated not just by commentators, but also by courts and other international bodies, which have repeated factual assumptions made without the benefit of input from the UK or US Governments, or understanding of the true position. The IPT, Commissioner and other independent UK bodies have confirmed this (as set out below). The Court should not proceed on the basis of such mischaracterisations. See further **§§1.1-1.28** below.

The Intelligence Sharing Regime

10. The Applicants' case challenges the UK's receipt of foreign intercept data collected by the US under the legal authority of s.702 Foreign Intelligence Surveillance Act 1978 ("FISA") (See Annex 2), pursuant to the "Prism" and "Upstream" programmes. The Applicants seriously mischaracterise the Prism and Upstream programmes. Neither Prism nor Upstream entails bulk interception by the US. Moreover, both programmes entail a detailed, recorded and audited process identifying particular selectors, such as phone numbers or email addresses, before interception can occur. In other words, they are targeted capabilities (see **§§1.1-1.18**). So far as the UK is concerned, it receives intelligence from the US and a range of other States. Before the IPT, Mr Charles Farr made a witness statement (See Annex 3) dealing with a range of factual matters and providing such explanations and descriptions of the Regimes as could be provided in open. As he explains, (a) receipt of foreign intelligence is vital to the protection of the public and provides intelligence not available from any other source and (b) it is not possible to distinguish between foreign intercept intelligence

and foreign intelligence derived in whole or in part from other sources (see **§§1.15-1.18**).

11. The detail of the domestic law and practice comprising the Intelligence Sharing Regime is set out in the body of the Observations (see **§§2.1-2.41**). As already noted, it comprises primary legislation based around the key Convention safeguards of necessity and proportionality - the SSA (See Annex 4) and the ISA (See Annex 5), as read with the CTA (See Annex 6); the HRA (See Annex 7); the DPA (See Annex 8); and the OSA (See Annex 9). That is supplemented by the Code (See Annex 10); and by internal arrangements (which are required to be made under the statutes governing each of the Intelligence Services). There is oversight by the ISC, the Commissioner and (as these cases demonstrate) the IPT.

The s.8(4) Regime

12. 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". It is described in general terms by the Commissioner in his Annual Reports of 2013 (See Annex 11) and 2014 (See Annex 12); in a report of the Intelligence and Security Committee of Parliament ("ISC") of 17 March 2015, *"Privacy and Security: A modern and transparent legal framework"* ("the ISC Report") at §§49-77 (See Annex 13); and in a report of the Investigatory Powers Review of June 2015 by David Anderson QC, *"A Question of Trust"* ("the Anderson Report") at chapter 10 (See Annex 14). All have been able to investigate the interception capabilities of the Intelligence Services in detail, with the full cooperation of the Services. Each has engaged with, or taken evidence from, many interested parties outside government, including some of the Applicants in this case, for the purposes of drafting their Reports. The Government can confirm the factual accuracy of the Reports' accounts of the Intelligence Services' capabilities (see **§§1.19-1.40**).

13. This ability and the manner in which it is operated is vital for the protection of national security. The s.8(4) Regime is critical to the discovery of threats and of targets who may be responsible for threats. That is particularly so given that, for

obvious reason, the Government does not have the same capabilities or intelligence opportunities in relation to external communications. The importance of the s.8(4) Regime is clear and has been acknowledged by the ISC, the Commissioner and David Anderson QC (see **§§1.29-1.35**). 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"*: §77(K). David Anderson QC identified example case studies (see **§1.34**) which speak for themselves in terms of the importance of some of the intelligence derived from this Regime.

14. The s.8(4) Regime involves "bulk" interception. However, that is because that is the only practical way of obtaining access to the necessary data. Both resource and practical/technical issues dictate how the interception is done. The Commissioner's Annual Report of 2013 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[4]: *"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."* (see **§1.33**)

15. Again, the Applicants significantly overstate their case. This is not, on any view, "mass surveillance". Nor is it "generalised access"; or targeting without suspicion. Any suggestion to the contrary is wrong. As is explained in more detail below, there are important limitations that lead to the position in which only the bearers which are most likely to yield valuable intelligence are even selected for interception. There is then a series of other selectors that limit and restrict the data subject to interception. And of that selection, only a small fraction is then ever selected for possible examination by an analyst. Such ultimate selection for examination is carefully controlled under the Regime, including specifically by reference to the concepts of necessity and proportionality. As the ISC correctly concluded at §77 of

[4] [***See Annex 11***]

its Report, the communications selected for examination *"are only the ones considered to be of the highest intelligence value. Only the communications of suspected criminals or national security targets are deliberately selected for examination."*(see **§§1.21-1.25**)

16. The true position is summarised by 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."* (**§1.28**)

This is not, on any view, "mass surveillance". Nor is it "generalised access"; or targeting without suspicion.

17. So far as concerns domestic law and practice, the key legislation is RIPA. It contains a series of important and stringent safeguards. It is supplemented by the Code and by internal arrangements (see **§§2.42-2.104**). There is again oversight by the ISC, the Commissioner and the IPT – as described in detail below at **§§2.105-2.124**.

Article 8: the Intelligence Sharing Regime (Question 1)

Victim status

18. The Applicants are not "victims" for the purposes of Art. 34 ECHR, applying the principles in *Zakharov v Russia* app. 47143/06, 4 December 2015 (Grand Chamber). They do not belong to any group of persons possibly affected by the Intelligence Sharing Regime. They put forward no basis on which their communications are at realistic risk of being intercepted under the Prism or Upstream programmes, and shared with the Intelligence Services; and they do not assert that this has in fact happened (see **§§3.1-3.7**).

In accordance with the law[5]

19. The Intelligence Sharing Regime is in accordance with the law for the purposes of Article 8(2) ECHR. The statutory provisions in the Intelligence Sharing Regime provide domestic law powers (and the basis) for the obtaining and subsequent use of communications and communications data. Those provisions are clearly "accessible" (see **§3.10**).

20. The Intelligence Sharing Regime is also sufficiently "foreseeable" (see **§§3.11-3.21**). In this context, the essential test 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: see §68 of *Malone v UK* (app. 8691/79), Series A no.82. 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.

21. **First**, the regime is sufficiently clear as regards the circumstances in which the Intelligence Services can in principle **obtain** information from the US authorities, which has been gathered under the Prism or Upstream programmes (see **§§3.11-3.16**). 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, 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. 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

[5] No separate issue arises as to 'necessity' of the Intelligence Sharing Regime, and no submissions are made about it by the Applicants.

Services). In particular, the Code provides a series of detailed public safeguards on obtaining information.

22. **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 (see **§§3.17-3.21**). Handling and use is addressed by (i) s. 19(2) of the CTA, as read with the statutory definitions of the Intelligence Services' functions (in s. 1 of the SSA and ss. 1 and 3 of ISA); (ii) the general proportionality constraints imposed by s. 6 of the HRA and - as regards retention periods in particular - the fifth data protection principle; and (iii) the seventh data protection principle (as reinforced by the criminal offence in ss. 1(1) and 8(1) of the OSA) as regards security measures whilst the information is being stored. Further, ss. 1-2 of the SSA and ss. 1-2 and 3-4 of the ISA, as read with ss. 19(3)-(5) of the CTA and s. 6(1) of the HRA, sufficiently address the circumstances in which the Intelligence Services may disclose information obtained from a foreign intelligence agency to others. In addition, 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. 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.

23. **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 (see **§§3.22-3.27**). The relevance of oversight mechanisms in the assessment of foreseeability, and in particular the existence of adequate safeguards against abuse, is well established in the Court's

case law: see e.g. *Kennedy*: when considering the general ECHR-compatibility of the RIPA s. 8(1) regime, the Court at §§155-170 of *Kennedy* "*jointly*" considered the "*in accordance with the law*" and "*necessity*" requirements, and in particular analysed the available oversight mechanisms (at §§165-168) in tandem with considering the foreseeability of various elements of the regime (§§156-164). See too the Grand Chamber's judgment in *Zakharov*, where the Court examined *"with particular attention"* the supervision arrangements provided by Russian law, as part of its assessment of the existence of adequate safeguards against abuse: §§271-280.

24. **Finally**, having regard to the core purpose of the in accordance with the law requirement as identified eg in *Malone,* it is important to note 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[6], and that the Regime as a whole (with the benefit of the Disclosure, now mirrored in the Code) is in accordance with the law (see **§3.28**). 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 an important strand of protection for the purposes of rights under the Convention.

25. These were the conclusions of the IPT after its careful examination of the issues (see **§1.45**). It is submitted that there is no reason for the Court to reach any different view.

The s.8(4) regime (Question 2)

Victim status

26. As is the case in respect of the Intelligence Sharing Regime (see §18 above), the Applicants are not "victims" applying the principles in *Zakharov* (save for the two

[6] 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." (See Annex 15)*

organisations who received a declaration in the IPT proceedings[7]). The Applicants cannot demonstrate that they are at realistic risk of selection/examination under the s.8(4) Regime i.e. that they have reason to believe their communications are of interest to the Intelligence Services on the grounds mentioned in s.5(3)(a), (b) or (c) (in the interests of national security, for the purposes of preventing or detecting serious crime or for the purpose of safeguarding the economic well-being of the United Kingdom) (see §4.1 below).

Lawfulness of the s.8(4) Regime

27. There is no good reason for the ECtHR to reach any different conclusion than it reached on the lawfulness of the parallel regime for the interception of communications under s.8(1) RIPA in *Kennedy v UK (*app. 26839/05, 18 May 2010). The IPT has also examined the issue of the lawfulness of the s.8(4) Regime with conspicuous care; and it is submitted reached the correct conclusion that the Regime was in accordance with law applying the Court's jurisprudence (**§§1.46-1.47**). The s.8(4) Regime satisfies the "in accordance with the law" and "necessity" tests.

In accordance with the law

28. The statutory provisions of RIPA provide domestic law powers for the regime. The "accessibility" requirement is satisfied in that RIPA is primary legislation 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 (**§4.32**).

29. As to foreseeability, the ECtHR has set out at §95 of *Weber and Saravia v Germany,* (dec.), app. 54934/00, ECHR 2006-XI ("*Weber*") the six "minimum safeguards" that the domestic legal framework needs to set out in the context of the interception of communications ("the *Weber* criteria") (see **§4.35**). *"[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*

[7] i.e. Amnesty International and the Legal Resources Centre – see §1.50 and §§4.100-4.108 below.

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). Each of the *Weber* criteria is satisfied by the Regime **(see §§4.40-4.55 below)**. See also *Kennedy* at §§155-167.

30. In relation to interception of the content of communications:

***(1) The "offences" which may give rise to an interception order*:** This requirement is satisfied by s. 5 of RIPA, as read with the relevant definitions in s.81 of RIPA and §§6.11-6.12 of the Code. This follows, in particular, from a straightforward application of §159 of *Kennedy*, and §133 of *RE v United Kingdom* (see **§4.40** and see further below at **§§3.13-3.15** and **§§4.77-4.81** as regards the meaning of "national security").

***(2) The categories of people liable to have their 'telephones tapped'*:**
As is clear from §97 of *Weber*, this second requirement in §95 of *Weber* applies <u>both</u> 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) (see **§4.41**).

As regards the *interception* stage (see **§4.42**):

(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. The term "external communication" is sufficiently defined in s. 20 and §5.1 of the Code (see **§§4.66-4.76** 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 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"[8]. Similarly, during the Parliamentary debate on the Bill that was to become RIPA, Lord Bassam referred to intercepting the whole of a communications "link".

(4) In addition, a s. 8(4) warrant may in principle authorise the interception of internal communications insofar as that is necessary in order to intercept the external communications to which the s. 8(4) warrant relates. See s. 5(6) of RIPA, and the reference back to s. 5(6) in s. 8(5)(b) of RIPA (which latter provision needs to be read with s. 8(4)(a) of RIPA). This point was also made clear to Parliament and it has in any event been publicly confirmed by the Commissioner.

(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, the s. 8(4) regime sufficiently identifies the categories of people who are liable to have their communications intercepted.

As regards the *selection* stage (see **§4.43**):

(1) No intercepted material (whether external or not) 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.

(2) As regards the former, 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 §159-160 of *Kennedy*.

(3) 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 listened to according to a factor which is (a) referable to an individual who is known to be for the time being in the British Islands and (b) which has as its purpose, or one of its purposes, the identification of material contained in communications sent by him or

[8] See the 5 December Judgment at §93. See too, for example, the ISC Report.

intended for him.

(3) Limits on the duration of 'telephone tapping': 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 **§§4.49-4.50** below, §161 of *Kennedy,* and the specific provisions for renewal of a warrant contained in §§6.22-6.24 of the Code[9].

(4)-(5) The procedure to be followed for examining, using and storing the data obtained; and the precautions to be taken when communicating the data to other parties**: (see §§4.51-4.53)**

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).

As regards the intercepted material that can be read, looked at or listened to pursuant to s.16 (and the certificate in question), the applicable regime is 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, before any material can be examined at all, the person examining it 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

[9] 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".*

reduce the extent of that intrusion. See Code, §§7.14-7.16.

(2) The Code affords further protections to material examined under the s.8(4) Regime at §§7.11-7.20. Thus, material should only be examined 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) sets out the precautions to be taken when communicating intercepted material that can be read, looked at or listened to pursuant to s. 16 to other persons (including foreign intelligence agencies: see §3.109 above). 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. 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.

(5) The detail of the s. 15 and s.16 arrangements is kept under review by the Commissioner (see §§2.79-2.81 and 2.97-2.98 below).

(6) The circumstances in which recordings may or must be erased or the tapes destroyed **(see §§4.54-4.55)**

Section 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.

31. The acquisition of **communications data** has rightly been 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 (see **§§4.29-4.31**). For that reason, the *Weber* criteria do not apply to the acquisition of communications data (and have never been held by the ECtHR so to apply). The applicable test is simply whether the law gives the individual adequate protection against arbitrary interference. The s.8(4) Regime satisfies that test. In any event if, contrary to the above, the *Weber* criteria apply to communications data, they are met (see **§§4.60-4.61**)

(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. 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 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, if a processing system was able to extract or generate a structured index of the

contents of a communication, it would be "metadata"; but would be content for the purposes of the s.8(4) Regime. Extracting 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 **§§4.41-4.43** below, 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 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.

(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. This is for the simple reason that obtaining this information would very obviously serve none of the authorised purposes in s. 15(4), and would not be in pursuance of any of the Intelligence Services' statutory functions. There is nothing unique about communications data (even when aggregated) here.

(5) Further, there is good reason for s. 16 of RIPA covering access to intercepted material (*i.e.* the content of communications) and not covering access to communications data (see the Applicants' complaints at §46(1) of their Additional Submissions). In order for s. 16 to work as a safeguard in relation

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

(6) The regime equally contains sufficient clear provision regarding the subsequent handling, use and possible onward disclosure by the Intelligence Services of related communications data.

32. None of the principal criticisms of the regime made by the Applicants (the scope of "external communications", the meaning of "national security", and the fact that warrants are not issued by judges) is well-founded, or prevents the Regime being "in accordance with the law". The concepts of "external communications" and "national security" are properly used and sufficiently precise: see **§§3.13-3.15, §§4.77-4.81 and §§4.42, §§4.66-4.76** below. As to the contention that prior judicial authorisation is necessary (see **§§4.96-4.99**):

(1) The Government strongly deny that the Convention requires or should require any such precondition. 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.

(2) The Court's case law does not require independent authorisation of warrants as a precondition of lawfulness, provided that the applicable regime otherwise contains sufficient safeguards. 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: 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:

"The Court recalls that in Dumitru Popescu (cited above, §§70-73) it expressed the view that either the body issuing authorisations for interception should be independent or there should be control by a judge or an independent body over the issuing body's activity. Accordingly, in this field, control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception, warranting close scrutiny (see Klass and others, cited above, §§42 and 55). The ex ante authorisation of such a measure is not an absolute requirement per se, because where there is extensive post factum judicial oversight, this may counterbalance the shortcomings of the authorisation (see Kennedy, cited above, §167)." (Emphasis added)

(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 Court's case law.)

(3) There is extensive independent (including judicial) *post factum* oversight of secret surveillance under the s.8(4) Regime. 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 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."

(4) Moreover, the following additional points about the applicable *post factum* independent oversight should also be made. 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. 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. The extent of his post factum oversight is illustrated (for example) by the detail of his 2013 Annual Report, which specifically addressed issues raised in this Application. 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, [See Annex 13]).

(5) Finally, the Applicants seek to place reliance on the CJEU judgment in *Digital Rights Ireland (See Annex 16)*. That case did not on any view purport to lay down minimum procedural safeguards under EU law. Nor did it purport to alter, expand or develop Convention jurisprudence (on the contrary, it referred to and purported to apply that jurisprudence – although it is notable that it simply did not consider or apply much of the relevant Convention jurisprudence). The CJEU has in any event been invited to consider the issues again following the reference made to it by the English Court of Appeal in *R (Davis and Watson) v Secretary of State for the Home Department* (see **§§4.17-4.28**) (See Annex 17)

Necessity

33. The s.8(4) Regime clearly satisfies the "necessity" test, not least given the State's margin of appreciation in this area (see **§§4.84-4.95**). It is subject to sufficient safeguards against abuse (for all the reasons already given with regard to the "in accordance with the law" test). It is also essential if the Intelligence Services are both

to discover and to address national security threats effectively. As the findings in the ISC and Anderson Reports indicate, it has enabled the discovery and successful disruption of major threats, in circumstances where interception under the regime was the only means likely to produce the necessary intelligence. 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 bearer are intercepted, even though only a tiny fraction of intercepted communications are ever, and can ever be, selected for potential examination, let alone examined. On a proper analysis, it does not.

Article 10 and NGO's (Questions 3 and 4)

34. The potential for confidential NGO material to be intercepted in the course of the operation of the s.8(4) Regime does not affect the correctness of the analysis summarised above (see **§§5.1-5.4**). Nor does the engagement of Article 10 in respect of such material give rise to a requirement for additional safeguards beyond those required by Article 8 (see **§§6.1-6.39**). The cases to which the Court has referred in its question – *Nordisk Film*[10], *Financial Times Ltd*[11], *Telegraaf Media* and *Nagla* – are all cases concerned with targeted measures directed to the identification and/or disclosure of journalistic sources. None of them is concerned with strategic monitoring of the type conducted under the s.8(4) Regime. In particular, there is no requirement for prior judicial authorisation in respect of the interception of NGO material under the s.8(4) Regime.

Article 6 (Question 5)

35. The domestic IPT proceedings in *Liberty* did not involve the determination of "civil rights and obligations" within the meaning of Article 6(1). There is a clear and consistent line of ECtHR authority which makes clear that the rights at issue in the field of secret interception powers are not "civil" rights (see **§§7.1-7.10**). In the alternative, even if Art. 6 did apply to the proceedings before the IPT, it was satisfied.

[10] *Nordisk Film & TV A/S v Denmark* App. No. 40485/02, 8 December 2005.
[11] *Financial Times Ltd and Others v the United Kingdom*, App. No. 821/03, 15 December 2009; (2010) 50 EHRR 1153.

Looked at as a whole, the IPT's procedures plainly did not impair the very essence of the applicants' right to a fair trial, particularly given the Court's conclusions in *Kennedy v United Kingdom* (see **§§7.11-7.50**) .

Article 14 (with Articles 8 and/or 10)

36. As to the assertion that the s.8(4) regime is indirectly discriminatory on grounds of nationality contrary to Article 14 ECHR (see **§§8.1-8.16**):

(1) The operation of the s.8(4) Regime does not mean that persons outside the United Kingdom are disproportionately likely to have their private communications intercepted. The Applicants' case is factually incorrect.

(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. The Secretary of State must certify that it is necessary to examine intercepted material by reference to a factor referable to such a person. To that extent, persons are treated differently on the basis of current location.

(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.

1 PART I - THE FACTS

1.1 The intelligence gathering activities and capacities of the UK, and the nature of interception programmes in the UK and US, have been widely mischaracterised as a result of the Snowden allegations. A number of mischaracterisations and inaccuracies have found their way into court judgments in proceedings to which neither the UK nor US governments were parties, or into texts of international institutions into which neither the UK nor US governments have had input. There, they have been presented as established fact, when they are anything but. Those errors are repeated by the Applicants and Intervenors in this case.

1.2 The difficulty of addressing such errors is compounded because it has been the policy of successive UK Governments to neither confirm nor deny ("NCND") assertions, allegations or speculation in relation to the Intelligence Services. By its very nature, the work of the Intelligence Services provides the paradigm example of a context where secrecy is required if the work is to be effective, and there is an obvious, and widely recognised, need to preserve that effectiveness. This means, as a general rule, the Government will adopt a position of NCND when addressing the Services' precise activities and capabilities. So it is only possible to address mischaracterisations in open to a limited extent.

1.3 That having been said, there are reports in which the activities and capabilities of the Intelligence Services are addressed, where the authors have taken evidence from the Intelligence Services, and which the Government can confirm are factually accurate. Those are a report of the Intelligence and Security Committee of Parliament ("ISC") of 17 March 2015[12], *"Privacy and Security: A modern and transparent legal framework"* ("the ISC Report"); a report of the Investigatory Powers Review of June 2015 by David Anderson QC, *"A Question of Trust"* ("the Anderson Report")[13]; and the regular annual (and now, twice-yearly) reports of the Commissioner. The US position as regards Prism and Upstream has also been set out by the US Executive Branch itself in various documents, as detailed below. The Court can rely upon those

[12] See [***Annex 13***]
[13] See [***Annex 14***]

sources. But otherwise, the Court cannot assume the truth of any of the broad factual assertions made in the Application, or indeed in submissions from the Intervenors, save where consistent with those Reports, and/or with material from the US Executive Branch; and it should not do so.

1.4 The most significant material factual errors asserted in the Application are addressed either in the "facts" section below, or in the body of the response to the Applicants' grounds, to the extent that the NCND principle allows them to be addressed. Separate and additional errors made by Intervenors will be addressed in the response to the interventions.

(1) The Prism/Upstream complaint

The Prism and Upstream programmes

1.5 The Applicants' case[14] challenges the UK's receipt of foreign intercept data collected by the US under the legal authority of s.702 Foreign Intelligence Surveillance Act 1978 ("FISA"), pursuant to the "Prism" and "Upstream" programmes. It is unnecessary for the Court to make detailed factual findings about the nature of the Prism and Upstream programmes, even if it were appropriate to do so, since the Applicants' case does not depend upon the precise nature of those programmes. However, it is important to observe that the consistent characterisation of these programmes as concerning "mass communications surveillance", both in the Application and in various submissions from interveners in this case, is simply wrong. The Applicants' broad characterisation of the nature of those programmes is flatly contradicted in a number of important respects by publicly available material, including from the US Government itself. No assumption can or should be made as to the truth of any of the Applicants' assertions, save where they are consistent with the US Government's own factual explanation.

1.6 By way of example, the Applicants assert that under Prism and Upstream, the two programmes provide for the *"bulk"* collection of *"vast amounts of communications and communications data carried by the submarine fibre optic cables passing through, into and*

[14] See "Additional Submissions on Facts and Complaints" at §§70-73.

out of the US" and that they are *"designed to capture the private communications of individuals across the globe"*: see Application Form Statement of Facts p4. This is wholly contrary to material from the US Government, contained in (i) a report of 18 April 2014 of the NSA Director of Civil Liberties and Privacy Office, *"NSA's Implementation of Foreign Intelligence Surveillance Act Section 702"*[15]; (ii) a paper from the Director of National Intelligence of 8 June 2013, *"Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act"*[16]; and (iii) a paper of 9 August 2013 from the NSA, *"The National Security Agency: Missions, Authorities, Oversight and Partnerships"*[17]. On the basis of that material, the position is rather that:

(1) The NSA's collection authorities stem from two key sources: Executive Order 12333 and FISA. All collection under any authority must be undertaken for foreign intelligence and counterintelligence purposes. Prism and Upstream are undertaken under the authority of FISA.

(2) Both Prism and Upstream require an NSA analyst to identify a specific non-US person located outside the US (e.g. a person belonging to a foreign terrorist organisation) as a "target", and to obtain a unique identifier associated with that target, such as an email address, to be used as a tasked "*selector*".

(3) The analyst must verify the connection between the target and the selector, and must document (a) the foreign intelligence information expected to be acquired; and (b) the information that would lead a reasonable person to conclude that the selector was associated with a non-US person outside the US. That documentation must be reviewed and approved or denied by two independent processes.

(4) Under Prism, service providers are compelled to provide the NSA with communications to or from such approved selectors. Under Upstream, service providers are required to assist the NSA lawfully to intercept communications to, from, or about approved selectors.

[15] See [***Annex 18***]
[16] See [***Annex 19***]
[17] See [***Annex 20***]

(5) Thus, neither Prism nor Upstream entails bulk interception. Moreover, both programmes entail a detailed, recorded and audited process identifying particular selectors, such as phone numbers or email addresses, before interception can occur[18].

(6) Both programmes are undertaken with the knowledge of the service provider, and under procedures approved by the FISA Court. All information obtained is based upon a written directive from the Attorney General and the Director of National Intelligence, detailing the foreign intelligence categories within which access requests must fall. Any such written directive is reviewed annually by the FISA Court.

(7) The NSA has a compliance programme, designed to ensure that its activities are conducted in accordance with law and procedure; therefore, in the case of Prism and Upstream, in accordance with s.702 FISA and associated requirements. Issues of non-compliance must be reported to the Office of the Director of National Intelligence and the Department of Justice for further reporting to the FISA Court and Congress, as required. ODNI and DOJ also regularly do audits of the NSA's compliance with targeting and minimisation procedures, including reviewing selectors used by the NSA.

1.7 The mischaracterisation of Prism and Upstream as involving "*bulk seizure, acquisition, collection and storage*" appears to result from a failure to distinguish between two different types of NSA programme. The NSA has indeed operated a programme which involved the collection of telephone call records, including the records of US citizens (but not the content of telephone conversations) in bulk. However, that programme was not Prism or Upstream. It was an entirely different programme, approved by the Foreign Intelligence Surveillance Court ("FISC") pursuant to section 215 of the USA Patriot Act (that section being replicated in FISA as section 501) ("the Section 215 Programme"). The US Privacy and Civil Liberties Oversight Board ("PCLOB"), an independent, bipartisan agency within the US government's executive branch, was tasked with investigating both the Section 215 Programme and collection under the authority of s.702 FISA (i.e. Prism/Upstream) in July 2013, following the Snowden allegations. In January 2014, it recommended that the Section

[18] See too the ISC's 17 July 2013 Statement at §4 (***See Annex 21***): *"Access under Prism is specific and targeted (not a broad "data mining" capability, as has been alleged*)".

215 Programme should end. The programme was subsequently ended by the USA Freedom Act, which was enacted in June 2015, and came into force on 29 November 2015 (See Annex 22).

1.8 PCLOB reached very different conclusions regarding Prism and Upstream. Its investigation of Prism and Upstream is substantially contained in a report of 2 July 2014, *"Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act"* ("PCLOB's 2 July Report"[19]). The Report summarised the nature of Prism and Upstream as follows at p.111, in terms which are entirely consistent with the position set out above:

> *"Unlike the telephone records program conducted by the NSA under Section 215 of the USA Patriot Act, the Section 702 program[20] is not based on the indiscriminate collection of information in bulk. Instead, the program consists entirely of targeting specific persons about whom an individualised determination has been made. Once the government concludes that a specific non-U.S. person located outside the United States is likely to communicate certain types of foreign intelligence information – and that this person uses a particular communications "selector", such as an email address or telephone number – the government acquires only those communications involving that particular selector.*
>
> *Every individual decision to target a particular person and acquire the communications associated with that person must be documented and approved by senior analysts within the NSA before targeting. Each targeting decision is later reviewed by an oversight team from the DOJ[21] and the ODNI[22] ("the DOJ/ODNI oversight team") in an effort to ensure that the person targeted is reasonably believed to be a non-US person located abroad, and that the targeting has a legitimate foreign intelligence purpose. The FISA Court does not approve individual targeting decisions or review them after they are made."*

1.9 PCLOB made 10 policy recommendations concerning the s.702 programme, in order to ensure protection of privacy rights. All of those recommendations have now been implemented in full or in part (see PCLOB's *"Recommendations Assessment Report"* of

[19] See [***Annex 23***]
[20] The "Section 702 program" includes both Prism and Upstream.
[21] The US Department of Justice
[22] The Office of the Director of National Intelligence

5 February 2016[23]). However, PCLOB's overall conclusion was that the s.702 programme (incorporating Prism/Upstream) was a lawful and valuable resource, consistent with US privacy rights under the Fourth Amendment. See e.g. p.9 of the 2 July Report:

> *"The Board also concludes that the core of the Section 702 program – acquiring the communications of specifically targeted foreign persons who are located outside the United States, upon a belief that those persons are likely to communication foreign intelligence, using specific communications identifiers, subject to FISA court-approved targeting rules and multiple layers of oversight – fits with the "totality of the circumstances" standard for reasonableness under the Fourth Amendment[24], as that standard has been defined by courts to date."*

1.10 The Government recognises that the Applicants' misunderstanding of the effect of the Prism and Upstream programmes is widely shared, and has been repeated by various courts or other bodies in Council of Europe States[25]. Nevertheless, it remains a clear misunderstanding.

1.11 An assertion that foreign nationals do not benefit from any protection for their privacy under US laws and practices is another mischaracterisation (albeit again, a widespread one). In fact, US law contains a number of protections for non-US persons whose communications may have been intercepted.

1.12 On 17 January 2014, the White House issued Presidential Policy Directive (PPD) no.28, which specifically extends privacy rights to non-US persons, stating:

---

[23] [***See Annex 24***]

[24] The Fourth Amendment to the US Constitution, incorporating the US constitutional right to privacy, states: *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*

[25] For example, the Advocate General in the recent CJEU case of *Schrems v Data Protection Commissioner C-362/14,* 6 October 2015 (***See Annex 25***) has asserted, it appears on the basis of findings made by the Irish High Court in proceedings to which the US Government was not party, that Prism "*allows the NSA unrestricted access to the mass data stored on servers located in the USA*": see [49] of the Advocate General's Opinion.

"All persons should be treated with dignity and respect, regardless of their nationality or wherever they may reside, and all persons have legitimate privacy interests in the handling of their personal information. US signals intelligence activities must, therefore, include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where that individual resides."

1.13 Pursuant to PPD 28, the US intelligence agencies were directed to adopt data protection policies and procedures, applying to the retention, use, maintenance and dissemination of information about non-US persons, "*to the maximum extent feasible consistent with national security…to be applied equally to the personal information of all persons, regardless of nationality*" (emphasis added). The agencies were required to report on adoption of such policies within a year, and have done so.

1.14 Quite irrespective of the important provisions of PPD 28, a number of provisions of s.702 FISA, and other US surveillance laws, have protected the privacy of non-US persons since before PPD 28 came into effect. The position as regards these protections is summarised in PCLOB's 2 July Report at pp. 98-100, which states, as far as material:

"A number of provisions of section 702 [FISA], as well as provisions in other US surveillance laws, protect the privacy of U.S. and non-U.S. persons alike. Those protections can be found, for example, in (1) limitations on the scope of authorised surveillance under Section 702; (2) damages and other civil remedies that are available to subjects of unauthorised surveillance as well as sanctions that can be imposed on government employees who engage in such conduct; and (3) prohibitions on unauthorised secondary use and disclosure of information acquired pursuant to the Section 702 program. These sources of statutory privacy protections are discussed briefly.

The first important privacy protection provided to non-US persons is the statutory limitation on the scope of Section 702 surveillance, which requires that targeting be conducted only for purposes of collecting foreign intelligence information. The definition of foreign intelligence information purposes is limited to protecting against actual or potential attacks; protecting against international terrorism, and proliferation of weapons

of mass destruction; conducting counter-intelligence; and collecting information with respect to a foreign power or foreign territory that concerns US national defense or foreign affairs. Further limitations are imposed by the required certifications identifying the specific categories of foreign intelligence information, which are reviewed and approved by the FISC. These limitations do not permit unrestricted collection of information about foreigners.

The second group of statutory privacy protections for non-US persons are the penalties that apply to government employees who engage in improper information collection practices – penalties that apply whether the victim is a US person or a non-US person. Thus, if an intelligence analyst were to use the Section 702 program improperly to acquire information about a non-US person (for example, someone with whom he or she may have had a personal relationship), he or she could be subject not only to the loss of his or her employment, but to criminal prosecution. Finally, a non-US person who was a victim of a criminal violation of either FISA or the Wiretap Act could be entitled to civil damages and other remedies…

The third privacy protection covering non-US persons is the statutory restriction on improper secondary use found at 50 USC §1806, under which information acquired from FISA-related electronic surveillance may not "be used or disclosed by Federal officers or employees except for lawful purposes"…

Further, FISA provides special protections in connection with legal proceedings, under which an aggrieved person – a term that includes non-US persons – is required to be notified prior to the disclosure or use of any Section 702-related information in any federal or state court. The aggrieved person may then move to suppress the evidence on the grounds that it was unlawfully acquired and/or was not in conformity with the authorising Section 702 certification. Determinations regarding whether the Section 702 acquisition was lawful and authorised are made by a United States District Court, which has the authority to suppress any evidence that was unlawfully obtained or derived.

Finally, as a practical matter, non-US persons also benefit from the access and retention procedures required by the different agencies' minimisation and/or targeting procedures. While these procedures are legally required only for US persons, the cost and difficulty of identifying and removing US person information from a large body of data means that

typically the entire dataset is handled in compliance with the higher US person standards."

The UK intelligence services' receipt of intelligence material from foreign states

1.15 Mr Farr's witness statement made in the IPT proceedings (see ***Annex 3*****)** at §§15-25 sets out the high degree of unlikelihood that any government can obtain all the intelligence it needs from its own activities; and the immense importance and value to the UK's national interest of its ability to receive intelligence from the US[26]. As he then notes at §25, "*intelligence derived from communications and communications data obtained from foreign intelligence partners, and from the US intelligence agencies in particular, has led directly to the prevention of terrorist attacks and serious crime, and the saving of lives*".

1.16 The point is not confined to intelligence from the US. The UK has bilateral intelligence sharing relationships with a number of countries, including Council of Europe states, which are of very great importance to its national security interests. See the Anderson Report at §§10.31-10.32:

"As discussed at 7.66 above, the strongest partnership is the Five Eyes community involving the UK, USA, Canada, Australia and New Zealand. But there is bilateral sharing with many countries, not all of them in the established communities of the EU or the North Atlantic Treaty Organisation (NATO). Some of these relationships are broadly based where there is an enduring mutual interest. Others come together for a particular purpose such as a joint intervention.

These intelligence relationships are a vital contributor to [the Intelligence Services'] ability to provide the intelligence that the Government seeks…"

1.17 Mr Farr §§29-30 goes on to explain why no workable distinction can be made between the sharing of intercept intelligence, and other forms of intelligence, such as

[26] See too §§10.29-10.32 of the Anderson Report.

intelligence from covert human sources, so that the former should be separately regulated:

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

1.18 GCHQ has obtained information from the US Government that the US Government obtained via Prism. The Government neither confirms nor denies that either the Security Service or the SIS has obtained from the US Government information obtained under Prism; or that any of the Intelligence Services have obtained from the US Government information obtained under Upstream. The reason for that NCND policy is that set out at Farr §§42-47.

Allegation of circumvention of domestic oversight regimes

1.19 Some of the intervenors have suggested (as if it were established fact) that receipt of intelligence material from the US via Prism and Upstream is used by the Intelligence Agencies as a means of circumventing domestic constraints on interception, imposed under RIPA[27]. That is entirely wrong. The Government has publicly confirmed that the receipt of such material is not and cannot lawfully be used as a means of circumventing domestic controls (see further below, under "Domestic Law and

[27] See e.g. the submissions of the International Commission of Jurists, pp. 3-4.

Practice"). Moreover, both the ISC and the Commissioner have stated on the basis of their own detailed investigations and sight of the evidence that this does not happen in practice. See the following (the effect of which is summarised at *Farr §§72-74, 124*):

(1) The ISC's Statement of 17 July 2013[28] on its investigation into the allegation that GCHQ used Prism as means of evading UK law (*"It has been alleged that GCHQ circumvented UK law by using the NSA's PRISM programme to access the content of private communications. From the evidence we have seen, we have concluded that this is unfounded"*).

(2) The Commissioner's 2013 Annual Report at §§6.8.1-6.8.6[29]. See in particular the question posed by the Commissioner and the unequivocal answer he gave at §6.8.1, together with his explanation at §6.8.6:
"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...
…
6.8.6 …information lawfully obtained by interception abroad is not necessarily available by interception to an interception agency here. In many cases it will not be available. If it is to be lawfully provided from abroad, it is sometimes appropriate for the interception agencies to apply explicitly by analogy the RIPA 2000 Part I principles of necessity and proportionality to its receipt here even though RIPA 2000 Part I does not strictly apply, because the interception did not take place in the UK by an UK agency. This is responsibly done in a number of appropriate circumstances by various of the agencies, and I am asked to review the consequent arrangements, although this may not be within my statutory remit."

1.20 To the extent that the Intervenors, or any sources that they cite, say otherwise, they speak without knowledge of the true position, and without the benefit of access to the evidence.

[28] See [***Annex 13***]
[29] See [***Annex 13***]

(2) The complaint about the alleged Tempora operation

The nature of interception under s.8(4) RIPA

1.21 The Government neither confirms nor denies the existence of the alleged Tempora interception operation, for the reasons set out at Farr §§42-47. However, 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 described in general terms by the Commissioner in his Annual Reports of 2013 and 2014; in a report of the Intelligence and Security Committee of Parliament ("ISC") of 17 March 2015[30], *"Privacy and Security: A modern and transparent legal framework"* ("the ISC Report")[31] at §§49-77; and in a report of the Investigatory Powers Review of June 2015 by David Anderson QC, *"A Question of Trust"* ("the Anderson Report")[32] at chapter 10. The Commissioner, the ISC and Mr Anderson QC are independent of Government. All have been able to investigate the interception capabilities of the Intelligence Services in detail, with the full cooperation of the Services[33]. Each has engaged with, or taken evidence from, many interested parties outside government, including some of the

[30] See [***Annex 14***]
[31] See [***Annex 13***]
[32] See [***Annex 14***]
[33] See e.g. the Commissioner's 2014 Report at §1.6 (***See Annex 12***):
"I can report that I have full and unrestricted access to all of the information and material that I require, however sensitive, to undertake my review. I am in practice given such unrestricted access and all of my requests (of which there have been many) for information and access to material or systems are responded to in full. I have encountered no difficulty from any public authority or person in finding out anything that I consider to be needed to enable me to perform my statutory function."
See e.g. the ISC Report, "Key Findings", p.1, (v) (***See Annex 13***):
"Our Inquiry has involved a detailed investigation into the intrusive capabilities that are used by the UK intelligence and security Agencies. This Report contains an unprecedented amount of information about those capabilities…" and p.11, §12: *"In carrying out this Inquiry, we are satisfied that the Committee has been informed about the full range of Agency capabilities, how they are used and how they are authorized. We have sought to include as much of this information as possible in this Report with the intention that it will improve transparency and aid public understanding of the work of the Agencies".*
See too the Anderson Report, p.1, §4 (***See Annex 14***):
"In conducting my Review I have enjoyed unrestricted access at the highest level of security clearance, to the responsible Government Departments (chiefly the Home Office and FCO) and to the relevant public authorities including police, National Crime Agency and the three security and intelligence agencies: MI5, MI6 and GCHQ. I have balanced those contacts by engagement with service providers, independent technical experts, NGOs, academics, lawyers, judges and regulators, and by fact-finding visits to Berlin, California, Washington DC, Ottawa and Brussels."

Applicants in this case[34], for the purposes of drafting their Reports. The Government can confirm the factual accuracy of the Reports' accounts of the Intelligence Services' capabilities.

1.22 The effect of this, as Mr Anderson QC stated at §§14.39-40 of his Report, is that the UK's current regime for bulk interception has now been *"exhaustively considered over the past year or so"* not only in his Report, but also by the Commissioner, ISC and IPT (in the Liberty proceedings), so that *"some of the most senior judicial and political figures in the country have had the opportunity to analyse the regime and comment upon it"*.[35] It should be added, this analysis and comment - by contrast to much speculation in the press and elsewhere - has been made on the basis of access to and evidence from the Intelligence Services themselves, and balanced appraisal of the Intelligence Services' capacities, considering evidence and representations from (in the ISC's words) "*both sides of the debate*".

1.23 A number of important factual matters need to be noted about s.8(4) interception. **First**, GCHQ could theoretically access traffic from a small percentage of the 100,000 "bearers" (i.e. fibre optic cables) making up the core structure of the internet. However, the resources required to process the data involved means that at any one time GCHQ in fact only accesses a fraction of that small percentage of bearers it has the ability to access. Those bearers GCHQ accesses are chosen exclusively on the basis of the possible intelligence value of the traffic they carry and are authorised for access by warrant. See the summary of the position at §§57—58 of the ISC Report (the Report is redacted for reasons of national security, and the redactions below are as they appear in the Report):

[34] See e.g. the Commissioner's extensive summary of his engagement with the public and interested parties in Chapter 3 of his 2014 Annual Report, "*Transparency and Accountability*". See also Annex 4 to the Anderson Report, and §§13-15 of the ISC Report (***See Annex 13***).

[35] That position may be contrasted, for instance, with the EU Parliament's Resolution of 12 March 2014, upon which the Applicants heavily rely in their Update Submissions (see the Update Submissions, §§9-12). The UK Government (in common with a number of Member States) did not engage with the inquiry preceding the Resolution, so that to the extent it reached any conclusions about the UK's interception capabilities, they were not based upon any evidence at all from the Intelligence Services, or access to information held by the Services.

"57. The allegation arising from the NSA leaks is that GCHQ "hoover up" and collect all internet communications. Some of those who gave evidence to this Inquiry said "the Agencies are monitoring the whole stream all the time", referring to the "apparent ubiquity of surveillance".

58. We have explored whether this is the case. It is clear that both for legal reasons and due to resource constraints it is not: GCHQ cannot conduct indiscriminate blanket interception of all communications. It would be unlawful for them to do so, since it would not be necessary or proportionate, as required by RIPA. Moreover, GCHQ do not have the capacity to do so and can only cover a fraction of internet communications.

- *Of the 100,000 "bearers" which make up the core infrastructure of the internet, GCHQ could theoretically access communications traffic from a small percentage (***). These are chosen on the basis of the possible intelligence value of the traffic they carry.*
- *However, the resources required to process the vast quantity of data involved mean that, at any one time, GCHQ access only a fraction of the bearers that they have the ability to access – around ***. (Again, these are chosen exclusively on the basis of the possible intelligence value of the traffic they carry).*
- *In practice, GCHQ therefore access only a very small percentage (around ***) of the internet bearers at any one time.*
- *Even then, this does not mean that GCHQ are collecting and storing all of the communications carried on these bearers…"*

1.24 Thus, the suggestion that GHCQ intercepts all communications entering and exiting the United Kingdom is simply wrong[36].

1.25 Specifically, 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 to identify those bearers that are most likely to contain external communications that will meet the descriptions of material certified for interception by the Secretary of State under s.8(4) RIPA: Farr §154. See too §6.7 of the Code (which requires this approach to be taken as a matter of law).

[36] See e.g. the Application Form Statement of Facts at §2(1), p4.

1.26 **Secondly**, GCHQ does not conduct "untargeted" surveillance of communications or communications data, intercepted pursuant to a s.8(4) warrant. (i.e. any selection of communications for examination is undertaken on the basis that they match selection rules used to find those communications of maximum intelligence interest). So, again, any suggestion that GCHQ engages in 'blanket' surveillance is wholly incorrect.

(1) One major processing system operated by GCHQ on all the bearers it has chosen to access under s.8(4) RIPA compares the traffic carried by the bearers against a list of specific "simple selectors" – that is, specific identifiers relating to an individual target, such as (for example) an email address. Any communications which match the selectors are automatically collected. All other communications are automatically discarded. See the ISC Report, §§61-63. As the ISC Report states at §64: *"In practice, 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"*.

(2) Another major processing system enables GCHQ to search for communications using more complicated criteria (for example, selectors with three or four different elements). This process operates against a far smaller number of bearers, which are chosen from the total number of bearers intercepted by GCHQ as those most likely to carry communications of intelligence interest: see the ISC Report, §§65-66.

(3) Under this second system, a set of "selection rules" is applied to communications travelling over a bearer. The system automatically discards the majority of traffic on the targeted bearers, which does not meet those rules (the filtering stage). There is then a further stage, before analysts can examine or read any communications (selection for examination). This involves GCHQ conducting automated complex searches, to draw out communications most likely to be of greatest intelligence value, which relate to GCHQ's statutory functions, and the selection of which meets conditions of necessity and proportionality. Those searches generate an index. Only

items contained in the index can potentially be examined by analysts. All other items cannot be searched for, examined or read. See the ISC Report, §§67-73.

(4) Thus, what is filtered out by the application of automated searches is immediately discarded and ceases to be available. As stated by the Commissioner at §6.5.55 of his 2013 Report[37]:
"What remains after filtering (if anything) will be material which is strongly likely to include individual communications which may properly and lawfully be examined under the section 8(4) process. Examination is then effected by search criteria constructed to comply with the section 8(4) process."

1.27 **Thirdly**, only a fraction of those communications selected for possible examination by either of the processing systems set out above is ever looked at by an analyst.

(1) In relation to communications obtained via the use of "simple selectors", a "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.

(3) In summary, as stated by the ISC, the communications selected for examination *"are only the ones considered to be of the highest intelligence value.*

[37] See [***Annex 11***]

Only the communications of suspected criminals or national security targets are deliberately selected for examination": see the ISC Report, §77.

1.28 That final observation is derived from 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."*

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

1.29 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[38] (see e.g. the Anderson Report at §10.22[39]):

(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, or to discovery of a threat; but that can only be done, if the Services have access to a substantial volume of communications through which to search for those links.

[38] See Mr Farr at §§143-147 for a summary of those differences.
[39] [***Annex 14***]

(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. 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.

1.30 In addition, there are technical reasons why it is necessary to intercept the 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 all the packets associated with that communication, and reassemble them.

1.31 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.

1.32 In summary, as Mr Farr stated at §149[40]:

> *"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."*

1.33 The Commissioner, the ISC Report, and the Anderson Report have all recently 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.

(1) The Commissioner's Annual Report of 2013 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[41]:

> *"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."*

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.

(2) The ISC Report stated as follows (see [***Annex 13***]):

[40] [***See Annex 3***]
[41] [***See Annex 11***]

"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))

"GCHQ have provided case studies to the Committee demonstrating the effectiveness of their bulk interception capabilities. Unfortunately, these examples cannot be published, even in redacted form, without significant risk to GCHQ's capabilities, and consequential damage to the national security of the UK. We can, however, confirm that they refer to complex problems relating directly to some of the UK's highest priority intelligence requirements." (§81)

"The examples GCHQ have provided, together with the other evidence we have taken, have satisfied the Committee that GCHQ's bulk interception capability is used primarily to find patterns in, or characteristics of, online communications which indicate involvement in threats to national security. The people involved in these communications may be already known, in which case valuable extra intelligence may be obtained (e.g. a new person in a terrorist network, a new location to be monitored, or a new selector to be targeted). In other cases, it exposes previously unknown individuals or plots that threaten our security which would not otherwise be detected.

L. We are satisfied that current legislative arrangements and practice are designed to prevent innocent people's communications being read. Based on that understanding, we acknowledge that GCHQ's bulk interception is a valuable capability that should remain available to them." (§§90, 90(L))

(3) The Anderson Report commented on the uses of bulk interception at §§7.22-7.27[42], noting the importance of bulk interception for target discovery; and observing that this did not mean suspicion played no part in the selection of communications channels for interception, or in the design of searches conducted on intercepted material. In particular:

[42] ***[See Annex 14]***

At §7.25, Mr Anderson QC stated:

> *"GCHQ explained that its bulk access capabilities are the critical enabler for the cyber defence of the UK, providing the vast majority of all reporting on cyber threats and the basis for counter-activity. In a recent two week period bulk access provided visibility to GCHQ of 96 distinct cyber-attack campaigns. Bulk access is also the only means by which GCHQ can obtain the information it needs to develop effective responses to these attacks."*

At §7.26, Mr Anderson QC stated in summary that it was for the courts to decide whether such bulk interception was proportionate, but that he was in no doubt about the value of its role:

> *"GCHQ provided case studies to the ISC to demonstrate the effectiveness of its bulk interception capabilities. I have been provided with the same case studies and with other detailed examples, on which I have had the opportunity to interrogate GCHQ analysts at length and by reference to detailed intelligence reports based on the analysis of bulk data. They leave me in not the slightest doubt that bulk interception, as it is currently practised, has a valuable role to play in protecting national security."*

(4) At §14.45, Mr Anderson QC concluded[43]:

> *"Whether or not the s.8(4) regime is proportionate for the purposes of ECHR Article 8 is an issue awaiting determination by the ECHR. It is not my function to offer a legal assessment, particularly in a case that is under*

[43] 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 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*". (See Annex 14)

consideration by a senior court. But on the basis of what I have learned, there is no cause for me either to disagree with the factual conclusions expressed in recent months by [the Commissioner], the IPT or the ISC, or to recommend that bulk collection in its current form should cease. Indeed its utility, particularly in fighting terrorism in the years since the London bombings of 2005, has been made clear to me through the presentation of case studies and contemporaneous documents on which I have had the opportunity to interrogate analysts and other GCHQ staff."

1.34 The Anderson Report contains (at Annex 9[44]) six "case study" examples of intelligence from the bulk interception of communications. The importance of those examples speaks for itself. 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");

[44] [***See Annex 14***]

(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").

1.35 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.

Internal and external communications

1.36 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, and see further below, under "domestic law and practice"). 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.

1.37 It was well understood by Parliament at the time RIPA was enacted that interception of a bearer for wanted external communications would necessarily entail the interception of at least some internal communications. See Lord Bassam of Brighton

(the relevant Government Minister) in the House of Lords in July 2000[45] (cited at Farr §130):

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

1.38 Nevertheless, 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 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.

1.39 The Commissioner's findings are entirely consistent with the above position: see his 2013 Annual Report at §§6.5.52-6.5.54:

> *"6.5.52 …I am satisfied from extensive practical and technical information provided to me that it is not at the moment technically feasible to intercept external communications without a risk that some internal communications may also be initially intercepted. This was contemplated and legitimised by s.5(6)(a) of RIPA 2000 which embraces*

[45] Lord Bassam of Brighton introduced the Regulation of Investigatory Powers Bill (i.e. the Bill that became RIPA) on behalf of the Government in the House of Lords. The quotation is from the Lords Committee, Hansard, 12 July 2000 at column 323. See [***Annex 26***]

"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."

6.6.53 Thus the unintended but unavoidable initial interception of some internal communications under a section 8(4) warrant is lawful. Reference to Hansard House of Lords Debates for 12 July 2000 shows that this was well appreciated in Parliament when the bill which became RIPA 2000 was going through Parliament.

6.5.54 However, the extent to which this material, lawfully intercepted, may be lawfully examined is strictly limited by the safeguards in [section 16 RIPA]…And in any event my investigations indicate that the volume of internal communications lawfully intercepted is likely to be an extremely small percentage of the totality of internal communications and of the total available to an interception agency under a section 8(4) warrant."

1.40 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 asserted that there is no practical distinction between internal and external communications and that the distinction has been "fundamentally eroded" and is "unclear"[46]. Those criticisms are 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 §§ 4.66-4.76.

(3) Proceedings in the IPT

[46] see §45 of the Applicants' Additional Submissions on the Facts and Complaints.

1.41 The Applicants brought claims in the IPT in 2013 ("the Liberty proceedings"), specifically challenging 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. While there are some minor differences between the allegations made in this Application and those made in the Liberty Proceedings, the IPT had the opportunity in the Liberty Proceedings to consider and rule upon the principal issues that the Applicants now raise.

1.42 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 he 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)).

1.43 Throughout the hearings, the claimants were represented by teams of experienced Counsel, and the IPT had the benefit of assistance from Counsel to the Tribunal. Following those hearings, the IPT issued a series of open judgments, as set out below.

Judgment of 5 December 2014

1.44 In its judgment of 5 December 2014 ("The 5 December Judgment"[47]) 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, but

[47] [See Annex 15]

assumed, 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[48]. The IPT adopted the shorthand "Prism issue" and "s.8(4) issue" for the matters arising under each head.

1.45 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) For the purposes of the "in accordance with the law" test, appropriate rules or arrangements governing intelligence sharing should exist and be publicly known and confirmed to exist, with their content sufficiently signposted; and they should be subject to proper oversight. However, they did not need to be in a code or statute: see judgment, §41.

(3) The IPT was entitled to look at the Intelligence Services' internal policies and procedures that were not made public – i.e. "below the waterline" - in order to determine whether the Intelligence Sharing regime offered adequate safeguards against abuse: see judgment, §50.

(4) Certain details of those internal policies and procedures could properly be made open without damaging national security. The respondents agreed to make voluntary disclosure of those details, which were recorded in the judgment ("the Disclosure"): see judgment, §§47-48. (The Disclosure is now reflected in the Code, the current version of which postdates the IPT's judgment. See in particular §§7.8-7.9 and chapter 12 of the Code.)

(5) The effect of the internal policies and procedures was that the same requirements and internal safeguards were applied to all data, solicited or unsolicited, received pursuant to Prism or Upstream, as applied to material obtained under RIPA by the Intelligence Services themselves: see judgment, §54.

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

(6) In sum, 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 §1.19(2), §3.24 and §3.26 above), and (iii) the Disclosure itself: judgment, §55.

(7) 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: see judgment, §154.

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

(1) The IPT first considered whether the difficulty of determining the difference between external and internal communications, whether as a theoretical or practical matter, was such as to render the s.8(4) regime not in accordance with the law. The answer was no: see judgment, §§93102.

(2) The requirement under s.16 RIPA that the Secretary of State certify the necessity of examining communications intercepted under a s.8(4) warrant, if they are to be examined using a factor referable to an individual known to be in the UK, was an important and adequate safeguard. It was also justified and proportionate not to extend that safeguard to communications data. The *Weber* criteria extend to communications data, but those criteria were met without reference to the safeguards in s.16 RIPA, and it was justified and proportionate to extend greater protection to the content of communications than to communications data: see judgment, §§103-114.

(3) The s.8(4) system, leaving aside the effect of s.16 RIPA, sufficiently complied with the *Weber* criteria[49], and was in accordance with the law. Moreover, the ECtHR's own conclusions on the oversight mechanisms under RIPA in *Kennedy* endorsed that conclusion: see judgment, §§117-140.

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

(4) 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: see judgment, §§141-148.

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

1.47 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

1.48 In a judgment of 6 February 2015 ("the 6 February Judgment")[50], 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.

[50] [***See Annex 27***]

Judgment of 22 June 2015

1.49 The IPT's judgment of 22 June 2015 ("the 22 June Judgment")[51] 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. The issue of "systemic proportionality" arose at this point because, if it was generally disproportionate e.g. to intercept the entirety of the contents of a fibre optic cable, all the claimants could in principle have been entitled to a remedy, on the basis that their communications of no intelligence interest would or might have been so intercepted, even if immediately discarded.

1.50 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[52]. 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[53] 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" for the purposes of Article 8 ECHR. However, they were not accessed after the expiry of the relevant time limit: see judgment, §14.

[51] [***See Annex 28***]

[52] The IPT's 22 June Judgment erroneously stated that the finding in favour of Amnesty International was a finding in favour of the Egyptian Initiative for Personal Rights. That mistaken attribution was corrected by the IPT in a letter of 2 July 2015 (See Annex 29).

[53] 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.

(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 procedure for selection of the communications for examination had in error not been followed. Accordingly, the selection of the communications for examination was not "in accordance with the law" for the purposes of Article 8 ECHR. Notwithstanding that, no use whatsoever had been made of any intercepted material, nor any record retained: see judgment, §15.

1.51 The IPT stated 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.*"

2 PART 2 - DOMESTIC LAW AND PRACTICE

The Intelligence Sharing Regime

2.1 The Intelligence Sharing Regime is contained principally in the following statutes, as supplemented by the Code (which itself reflects the IPT's 5 December and 6 February Judgments):

(1) the SSA and the ISA, as read with the CTA;
(2) the HRA;
(3) the DPA; and
(4) the OSA.

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

The SSA, the ISA and the CTA

2.2 Section 1 SSA provides in relevant part:

> *"(2) The function of the [Security] Service shall be the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means.*
> *(3) It shall also be the function of the [Security] Service to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands.*
> *(4) It shall also be the function of the [Security] Service to act in support of the activities of police forces, the National Crime Agency and other law enforcement agencies in the prevention and detection*[54] *of serious crime*."

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

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

See also s. 19(3) CTA.[55]

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

> *"(a) to obtain and provide information relating to the actions or intentions of*

[54] By s. 1(5) of the SSA, the definitions of "prevention" and "detection" in s. 81(5) of RIPA apply for the purposes of the SSA.
[55] By s. 19(3), information obtained by the Security Service for the purposes of any of its functions "*may be disclosed by it - (a) for the purpose of the proper discharge of its functions, (b) for the purpose of the prevention or detection of serious crime, or (c) for the purpose of any criminal proceedings*."

persons outside the British Islands; and

(b) to perform other tasks relating to the actions or intentions of such persons."

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

> "*The functions of the Intelligence Service shall be exercisable only –*
>
> *(a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or*
>
> *(b) in the interests of the economic well-being of the United Kingdom; or*
>
> *(c) in support of the prevention or detection of serious crime.*"

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

> *"... that there are arrangements for securing that no information is obtained by the Intelligence Service except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary –*
>
> *(i) for that purpose;*
>
> *(ii) in the interests of national security;*
>
> *(iii) for the purpose of the prevention or detection of serious crime; or*
>
> *(iv) for the purpose of any criminal proceedings ...*"

See also s. 19(4) CTA.[56]

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

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

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

…."

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

> "*(a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or*
>
> *(b) in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or*
>
> *(c) in support of the prevention or detection of serious crime*."

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

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

See also s. 19(5) of the CTA.[57]

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

2.11 By s. 19(2) CTA:

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

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

exercise of any of its other functions."

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

The HRA

2.12 Art. 8 ECHR is a "Convention right" for the purposes of the HRA: s. 1(1) HRA. Art. 10 of the ECHR is similarly a Convention right (and is similarly set out in Sch. 1 to the HRA).

2.13 By s. 6(1) HRA: "*It is unlawful for a public authority to act in a way which is incompatible with a Convention right*." Each of the Intelligence Services is a public authority for this purpose. Thus, when undertaking <u>any</u> activity that interferes with Art. 8 rights (such as obtaining communications or communications data, or retaining, using or disclosing such information), the Intelligence Services must (among other things) act proportionately, having regard to the legitimate aim pursued,[58] pursuant to s. 6(1) HRA. Further, the same obligation to act proportionately is imposed insofar as the contemplated activity interferences with Art. 10 rights.

2.14 Section 7(1) HRA provides in relevant part:

> "*A person who claims that a public authority has acted (or proposes to act) in a way which is made unlawful by section 6(1) may –*
>
> *(a) bring proceedings against the authority under this Act in the appropriate court or tribunal ....*"

The DPA

2.15 Each of the Intelligence Services is a "data controller" (as defined in s. 1(1) DPA) in relation to all the personal data (as defined in s. 1(1) DPA) that it holds.

[58] The permissible aims being specified in the SSA and the ISA, respectively.

2.16 As a data controller, each of the Intelligence Services is in general required by s. 4(4) DPA to comply with the data protection principles in Part I of Sch. 1 to the DPA. That obligation is subject to ss. 27(1) and 28(1) DPA, which exempt personal data from (among other things) the data protection principles if the exemption "*is required for the purpose of safeguarding national security*". By s. 28(2) DPA, a Minister may certify that exemption from the data protection principles is so required. Copies of the ministerial certificates for each of the Intelligence Services are available on request. Those certificates (see ***Annex 30***) certify that personal data that are processed in performance of the Intelligence Services' functions are exempt from the first, second and eighth data protection principles (and are also exempt in part from the sixth data protection principle). Thus the certificates do <u>not</u> exempt the Intelligence Services from their obligation to comply, *inter alia*, with the fifth and seventh data protection principles, which provide:

> "*5.Personal data processed*[59] *for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. …*
>
> *7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data*."[60]

2.17 Insofar as the obtaining of an item of information by any of the Intelligence Services from a foreign intelligence agency amounts to an interference with Art. 8 rights, that item of information will in general amount to personal data. Accordingly, when the Intelligence Services obtain any such information from a foreign intelligence agency, they are obliged by the DPA:

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

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

(2) to take appropriate technical and organisational measures to guard against unauthorised or unlawful processing of the data in question and against accidental loss of the data in question. (See also, in this regard, §2.19 below).

The OSA

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

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

RIPA

2.20 In general, and subject to the provisions of the Code (as to which see below), the Intelligence Services are not required to seek authorisation under RIPA in order to obtain communications or communications data from foreign intelligence agencies. However, this does not mean that RIPA is of no relevance in the present context.

2.21 In particular, not least given the safeguards and oversight mechanisms that Parliament saw fit to impose in the case of interception pursuant to a RIPA interception warrant (see §§3.71-3.144 below), and in the light of the well-established principle of domestic public law set out by the House of Lords in *Padfield v Ministry*

of Agriculture, Fisheries and Food [1968] AC 997[61], it would as a matter of domestic public law be unlawful for any of the Intelligence Services to deliberately circumvent those safeguards and mechanisms (and attempt to avoid the need to apply for an interception warrant under RIPA) by asking a foreign intelligence agency to intercept certain specified communications and disclose them to the Intelligence Services. (That is not to say that there will not be circumstances where there are legitimate reasons to ask a foreign intelligence agency to intercept particular communications, for example, where it is not technically feasible for the Intelligence Services themselves to undertake the interception in question.)

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

The Code

2.23 Chapter 12 of the Code[62] mirrors the effect of the Disclosure, recorded in the IPT's 5 December and 6 February Judgments[63]. Chapter 12 states as follows:

> ***"12 Rules for requesting and handling unanalysed intercepted communications from a foreign government***
>
> ***Application of this chapter***

[61] The principle in *Padfield* is that a statutory discretion must be used so as to promote, and not to thwart, the policy and object of the Act. The judgment is at [***See Annex 31***].

[62] [***See Annex 10***]

[63] A judicial decision of this type can be taken into account in assessing "foreseeability" for the purposes of Art. 8(2): *Uzun v. Germany* (2011) 53 EHRR 24, at §62. So, for the avoidance of doubt, prior to the issue of the (revised) Code on 15 January 2016, the domestic law position was the same, as the result of the 5 December and 6 February judgments (***See Annexes 15 and 27***).

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 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[64].

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."

2.24 In sum, the effect of the Code is to confirm that, in the factual premises relevant to the Liberty proceedings (and therefore to this Application), exactly the same internal safeguards governing use, disclosure, sharing, storage and destruction apply as a matter of substance to material obtained via intelligence sharing as apply to similar material obtained through interception under Part I of RIPA.

[64] 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."*

Other safeguards

2.25 The above statutory framework is underpinned by detailed internal guidance, including in the form of "arrangements" under s. 2 of the SSA and ss. 2 and 4 of the ISA, and by a culture of compliance. The latter is reinforced by the provision of appropriate mandatory training to staff within the Intelligence Services, and by vetting procedures to ensure that staff faithfully operate within the aims, safeguards and ethos of the Intelligence Services: see Mr Farr §§51-53.

Oversight mechanisms in the Intelligence Sharing Regime

2.26 There are two principal oversight mechanisms in the Intelligence Sharing Regime: the ISC; and the IPT.

The ISC

2.27 SIS and GCHQ are responsible to the Foreign Secretary,[65] who in turn is responsible to Parliament. Similarly, the Security Service is responsible to the Home Secretary, who in turn is responsible to Parliament. In addition, the ISC plays an important part in overseeing the activities of the Intelligence Services. In particular, the ISC is the principal method by which scrutiny by Parliamentarians is brought to bear on those activities.

2.28 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. The ISC has itself welcomed these changes in the JSA, and it considers that they are "broadly in line with" those that it had previously recommended to Government and which "increase accountability" [***See Annex 32***].

[65] 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).

2.29 The ISC consists of nine members, drawn from both the House of Commons and the House of Lords. Each member is appointed by the House of Parliament from which the member is to be drawn (they must also have been nominated for membership by the Prime Minister, following consultation with the leader of the opposition). No member can be a Minister of the Crown. The Chair of the ISC is chosen by its members. See s. 1 of the JSA. The current chair is The Rt Hon Dominic Grieve QC MP, a former Attorney General. The executive branch of Government has no power to remove a member of the ISC: a member of the ISC will only vacate office if he ceases to be a member of the relevant House of Parliament, becomes a Minister of the Crown or a resolution for his removal is passed by the relevant House of Parliament. See §1(2) of Sch. 1 to the JSA.

2.30 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 Mr Farr §71.

2.31 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 Mr Farr §66.

2.32 The ISC meets at least weekly whilst Parliament is sitting. It is supported by staff who have the highest level of security clearance: see Mr Farr §67. Following the extension to its statutory remit as a result of the JSA, the ISC's budget has been substantially increased: see Mr Farr §69.

2.33 The ISC must make an annual report to Parliament on the discharge of its functions (s. 3(1) of the JSA), and may make such other reports to Parliament as it considers

appropriate (s. 3(2) of the JSA). Such reports must be laid before Parliament (see s. 3(6)). They are as necessary redacted on security grounds (see ss. 3(3)-(5)), although the ISC may report redacted matters to the Prime Minister (s. 3(7)). The Government lays before Parliament any response to the reports that the ISC makes.

2.34 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 Mr Farr §70.

The IPT

2.35 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 (§1(1) of Sch. 3 to RIPA). The President of the IPT must hold or have held high judicial office (§2(2) of Sch. 3 to RIPA).

2.36 The IPT's jurisdiction is broad. As regards the Intelligence Sharing regime, the following aspects of the IPT's *jurisdiction* are of particular relevance. The IPT 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 (ss. 65(2)(a), 65(3)(a) and 65(3)(b) RIPA). The IPT may consider and determine any complaints by a person who is aggrieved by any conduct by or on behalf of any of the Intelligence Services which he believes to have taken place in relation to him, to any of his property, to any communications sent by or to him, or intended for him, or to his use of any telecommunications service or system (ss. 65(2)(b), 65(4) and 65(5)(a) RIPA). Complaints of the latter sort must be investigated and then determined "by applying the same principles as would be applied by a court on an application for judicial review" (s. 67(3) RIPA).

2.37 Thus the IPT has jurisdiction to consider any claim against any of the Intelligence Services that it has obtained information from a foreign intelligence agency in breach

of the ECHR or has disclosed information to a foreign intelligence agency in breach of the ECHR. Further, the IPT can entertain any other public law challenge to any such alleged obtaining or disclosure of information.

2.38 Any person, regardless of nationality, may bring a claim in the IPT[66] As a result, the IPT is perhaps one of the most far-reaching systems of judicial oversight over intelligence matters in the world.

2.39 Pursuant to s. 68(2) RIPA, the IPT has a broad power to require a relevant Commissioner (as defined in s. 68(8)) to provide it with assistance. Thus, in the case of a claim of the type identified in §3.48 above, the IPT may require the Intelligence Services Commissioner (see ss. 59-60 of RIPA) to provide it with assistance.

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

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

2. The s. 8(4) Regime

2.42 The s. 8(4) Regime is principally contained in Chapter I of Part I of RIPA and the Code, as elucidated in the IPT's 5 December Judgment[67], and the Commissioner's 2013 Annual Report. The s. 8(4) regime also incorporates aspects of the Intelligence Sharing regime addressed above.

[66] 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.

[67] A judicial decision of this type can be taken into account in assessing "foreseeability" for the purposes of Art. 8(2): *Uzun v. Germany*, app. 35623/05, ECHR 2010, at §62.

2.43 Section 71 RIPA imposes a duty on the Secretary of State to issue, following appropriate consultation, one or more codes of practice relating to the exercise and performance of the powers and duties conferred or imposed by or under Part I of RIPA (which includes ss. 1-19). Any person exercising or performing any power or duty under ss. 1-19 must have regard to any relevant provisions of every code of practice for the time being in force: s. 72(1). Further, where the provision of a code of practice appears to the Tribunal, a court or any other tribunal to be relevant to any question arising in the proceedings, in relation to a time when it was in force, that provision of the code must be taken account in determining that question. A similar duty is imposed on the Commissioner: see s. 72(4) RIPA. The code of practice can be taken into account in assessing "foreseeability" for the purposes of Art. 8(2): *Kennedy*, at §157. The current code of practice ("the Code") was issued on 15 January 2016[68]. The previous version was issued in July 2002 ("the 2002 Code"[69]).

The interception of communications under RIPA

2.44 S. 2 RIPA provides a detailed definition of the concept of "interception":

(1) By s. 2(2), interception occurs if (among other things) a person "modifies or interferes with" a telecommunications system so as to make "available" the content of a communication which is being transmitted on that system "to a person other than the sender or intended recipient of the communication". By s. 2(1), the term "telecommunications system" means: "... *any system (including the apparatus comprised in it) which exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy*."

(2) By s. 2(6), the "modification" of a telecommunications system includes "*the attachment of any apparatus to, or other modification of or interference with ... any part of the system*". Significantly, by s. 2(8):

"For the purposes of this section the cases in which any contents of a communication are to be taken to be made available to a person while being transmitted shall include

[68] [***See Annex 10)***]
[69] [***See Annex 33***]

any case in which any of the contents of the communication, while being transmitted, are diverted or recorded so as to be available to a person subsequently."

In other words, "interception" can merely comprise the obtaining and recording of the contents of a communication (as it is being transmitted) so as to make it "available" subsequently to be read, looked at or listened by a person. No-one in fact needs to have actually read, looked at or listened to the communication for interception to occur.

2.45 Under s. 1(1) RIPA it is an offence, punishable by a term of imprisonment of up to two years and a fine,[70] for a person intentionally and without lawful authority to intercept, at any place in the UK, any communication in the course of its transmission by means of a public telecommunications system. The Commissioner also has power to serve a monetary penalty notice (of up to £50,000) on a person who has intercepted a communication without lawful authority (in circumstances which do not amount to an offence under s. 1(1)), and who was not making an attempt to act in accordance with a warrant (see s. 1(1A)).

2.46 Conduct has lawful authority for the purposes of s. 1 if it takes place in accordance with a warrant under s. 5 RIPA: s. 1(5)(b). As in RIPA itself, such warrants will be referred to as "interception warrants".

The issuing of interception warrants

2.47 Interception warrants are issued by the Secretary of State under s. 5(1) RIPA. Such warrants must be authorised personally by the Secretary of State: s. 7 RIPA.

2.48 An application must be made before an interception warrant can be issued: s. 6(1) RIPA. Such an application may only be made by or on behalf of one of the persons listed in s. 6(2) RIPA (which list includes the Director-General of the Security Service, the Chief of SIS and the Director of GCHQ). The application must contain all the detailed matters set out in §6.10 of the Code[71] (and the position was exactly the same

[70] See s. 1(7).

[71] That is: (i) the background to the operation in question, including a description of the communications to be intercepted, details of the CSP(s) and an assessment of the feasibility of the operation where it is relevant, and a description of the conduct to be authorised; (ii) the certificate

under §5.2 of the 2002 Code). This ensures that the Secretary of State has the information he needs properly to determine, under the statutory tests, whether to issue an interception warrant. The Commissioner has confirmed that:

> *"... the paperwork is almost always compliant and of a high quality. If there are occasional technical lapses, these are almost always ironed out in the interception agencies themselves or in the Secretary of State's department before the application reaches the relevant Secretary of State."* (2013 Annual Report at §3.39[72])

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

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

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

2.51 The nature of the proportionality assessment that the Secretary of State should undertake before issuing a warrant is further expanded upon in §§3.6-3.7 of the Code. In particular, §3.7 of the Code explains that the following elements of proportionality should be considered:

> *"- balancing the size and scope of the proposed interference against what is sought to be achieved;*
> *- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;*

---

that will regulate the examination of intercepted material; (iii) an explanation of why the interception is considered to be necessary for one or more of the s.5(3) purposes; (iv) a consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct; (v) where an application is urgent, supporting justification; (vi) an assurance that intercepted material will be read, looked at or listened to only so far as it is certified and it meets the conditions of ss.16(2)-(6) RIPA; and (vii) an assurance that all material intercepted will be handled in accordance with the safeguards required by ss.15 and 16 RIPA.

[72] ***[See Annex 11]***

-considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result; and

-evidencing, as far as reasonably practicable, what other methods have been considered and were either not implemented or have been employed but which are assessed as insufficient to fulfil operational objectives without the addition of the intercept material sought."

(Broadly equivalent provisions were equally contained in §§2.4-2.5 of the 2002 Code.)

2.52 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[73] serious crime[74] 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.

2.53 The words "in circumstances appearing to the Secretary of State to be relevant to the interests of national security", which narrow purpose (c), were added to s.5(3) RIPA by the Data Retention and Investigatory Powers Act 2014 ("DRIPA") (See Annex 34), with effect from 17 July 2014. However, even prior to 17 July 2014, the 2002 Code similarly narrowed purpose (c) as regarded the s.8(4) Regime[75]. The Code states (and the 2002 Code stated) that the Secretary of State must consider whether the economic well-being of the UK which is to be safeguarded is, on the facts of the case, directly related to national security, and the Secretary of State cannot issue a warrant on s. 5(3)(c) grounds unless such a "*direct link*" has been established: see Code, §6.12.

2.54 A further limitation on purpose (c) is provided by s. 5(5) RIPA:

"*A warrant shall not be considered necessary [for the purpose of safeguarding the economic well-being of the United Kingdom, in circumstances appearing to the Secretary of State to be relevant to the interests of national security] unless the*

[73] The terms "preventing" and "detecting" are defined in s. 81(5) of RIPA.
[74] The term "serious crime" is defined in ss. 81(2)(b) and 81(3) of RIPA.
[75] This was the case under §5.4 of the Code in the version from July 2002. See now §6.12 of the Code.

information which it is thought necessary to obtain is information relating to the acts or intentions of persons outside the British Islands."

2.55 The Commissioner has confirmed that the Secretaries of State provide a real and practical safeguard:

> *"The Secretaries of State themselves are entirely conscientious in undertaking their RIPA 2000 Part I Chapter I duties. They do not rubber stamp applications. On the contrary, they sometimes reject applications or require more information."* [*2013 Annual Report at §3.40*]

2.56 Further, as regards s. 8(4) warrants in particular, the Commissioner found in §6.5.43 of his 2013 Annual Report:

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

2.57 All warrant applications under the s. 8(4) regime must be kept so that they can be scrutinised by the Commissioner: §6.27 of the Code (and to similar effect, §5.17 of the 2002 Code).

Section 8(4) warrants

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

"*(4) Subsections (1) and (2)*[76] *shall not apply to an interception warrant if-*

(a) the description of communications to which the warrant relates confines the conduct authorised or required by the warrant to conduct falling within subsection (5); and

(b) at the time of the issue of the warrant, a certificate applicable to the warrant has been issued by the Secretary of State certifying-

(i) the descriptions of intercepted material[77] *the examination of which he considers necessary; and*

(ii) that he considers the examination of material of those descriptions necessary as mentioned in section 5(3)(a), (b) or (c).

(5) Conduct falls within this subsection if it consists in-

(a) the interception of external communications in the course of their transmission by means of a telecommunication system; and

(b) any conduct authorised in relation to any such interception by section 5(6).

(6) A certificate for the purposes of subsection (4) shall not be issued except under the hand of the Secretary of State."

2.59 The term "*communication*" is defined broadly in s. 81(1) RIPA to include (among other things) "*anything comprising speech, music, sounds, visual images or data of any description*". The term "*external communication*" is defined in s. 20 to mean "*a communication sent or received outside the British islands*". In addition, §6.5 of the Code provides (and §5.1 of the 2002 Code was to similar effect):

"*External communications are defined by RIPA to be those which are sent or received outside the British Islands. They include those which are both sent and received outside the British Islands, whether or not they pass through the British Islands in course of their transmission. They do not include communications both sent and received in the British Islands, even if they pass outside the British Islands en route. For example, an email from a person in London to a person in Birmingham will be an internal, not an external, communication for the purposes of section 20 of RIPA, whether or not it is routed via IP addresses outside the British Islands, because both the sender and intended recipient are within the British*

[76] See §2.68 below.

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

Islands."

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

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

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

> "*The conduct authorised by an interception warrant shall be taken to include –*
>
> *(a) all such conduct (including the interception of communications not identified by the warrant) as it is necessary to undertake in order to do what is expressly authorised or required by the warrant;*
>
> *(b) conduct for obtaining related communications data*[78]*;...*"

2.62 The reference in s. 5(6)(a) to "*communications*" as opposed to "*external communications*" is to be noted. In particular, s. 5(6)(a) makes clear that the conduct authorised by a s. 8(4) warrant may <u>in principle</u> include the interception of internal communications insofar as that is necessary in order to intercept the external communications to which the warrant relates.

2.63 When the Secretary of State issues a s.8(4) warrant, it must be accompanied by a certificate in which the Secretary of State describes the intercepted material that may be examined, and certifies that he considers examination of that material to be necessary for one or more of the purposes in s.5(3) RIPA: see s.8(4)(b) RIPA and §6.14 of the Code. The Code further states at §6.14[79]:

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

[79] See also §6.3 of the 2002 Code.

"The purpose of the statutory certificate is to ensure that a selection process is applied to intercepted material so that only material described in the certificate is made available for human examination. Any certificate must broadly reflect the "Priorities for Intelligence Collection" set by the NSC for the guidance of the intelligence agencies. For example, a certificate might provide for the examination of material providing intelligence on terrorism (as defined in the Terrorism Act 2000) or on controlled drugs (as defined by the Misuse of Drugs Act 1971). The Interception of Communications Commissioner must review any changes to the descriptions of material specified in a certificate."

2.64 The Code states at §6.7:

"When conducting interception under a section 8(4) warrant, an intercepting agency must use its knowledge of the way in which international communications are routed, combined with regular surveys of relevant communication links, to identify those individual communications bearers that are most likely to contain external communications that will meet the descriptions of material certified by the Secretary of State under section 8(4). It must also conduct the interception in ways that limit the collection of non-external communications to the minimum level compatible with the objective of intercepting wanted external communications."

2.65 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). So in principle, it authorises the interception of all communications passing down a bearer or bearers.

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

2.67 Like all applications for s. 8(4) warrants, the warrants themselves (and their accompanying certificates) must be kept so as to be available to be scrutinised by the Commissioner: see §6.27 of the Code (and, to similar effect, §5.17 of the 2002 Code).

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

> "*(1) An interception warrant must name or describe either-*
>
> *(a) one person as the interception subject; or*
>
> *(b) a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place.*
>
> *(2) The provisions of an interception warrant describing communications the interception of which is authorised or required by the warrant must comprise one or more schedules setting out the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying the communications that may be or are to be intercepted.*
>
> *(3) Any factor or combination of factors set out in accordance with subsection (2) must be one that identifies communications which are likely to be or to include-*
>
> *(a) communications from, or intended for, the person named or described in the warrant in accordance with subsection (1); or*
>
> *(b) communications originating on, or intended for transmission to, the premises so named or described*."

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

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

2.70 Section 16(1) imposes the requirement that:

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

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

(b) falls within subsection (2)."

2.71 Given the definition of "intercepted material", s. 16(1) applies both to external communications and to any internal communications that may have been intercepted under a s. 8(4) warrant[80].

2.72 The Code expands upon the requirement in s.16(1) that before intercepted material is examined, it must have been certified as necessary to examine it for one of the statutory purposes in s.5(3) RIPA: see Code, §6.14, and §3.76 above.

2.73 The Commissioner must review any changes to the descriptions of material specified in a certificate: see Code, §6.14.

2.74 Section 16(2) provides in relevant part:

> "*…intercepted material falls within this subsection so far only as it is selected to be read, looked at or listened to otherwise than according to a factor which-*
>
> *(a) is referable to an individual who is known to be for the time being in the British Islands; and*
>
> *(b) has as its purpose, or one of its purposes, the identification of material contained in communications sent by him, or intended for him*."

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

> "*(3) Intercepted material falls within subsection (2), notwithstanding that it is selected by reference to any such factor as is mentioned in paragraph (a) and (b) of*

[80] Section 20 RIPA defines "intercepted material", in relation to an interception warrant, as *"the contents of any communications intercepted by an interception to which the warrant relates"*. Thus, it includes internal as well as external communications intercepted pursuant to the warrant.

that subsection, if-

(a) It is certified by the Secretary of State for the purposes of section 8(4) that the examination of material selected according to factors referable to the individual in question is necessary as mentioned in subsection 5(3)(a), (b) or (c); and

(b) The material only relates only to communications sent during a period specified in the certificate that it no longer than the permitted maximum[81]."

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

2.77 Thus, the s. 8(4) regime envisages the following (which is also explained in the Code at §6.1, entitled "Section 8(4) interception in practice"[82]):

(1) A volume of intercepted material will be generated by the act of interception pursuant to a s. 8(4) warrant. The volume may <u>in principle</u> be substantial. Further, the intercepted material may be recorded so as to be available for subsequent examination (see s. 2(8) of RIPA).

(2) Pursuant to the s. 16 arrangements, a <u>much smaller</u> volume of intercepted material is then selected to be read, looked at or listened to by persons. The intercepted material so selected must be certified (in the Secretary of State's certificate) as material of a description that may be examined, and as material the examination of which is necessary as mentioned in s. 5(3)(a), (b) or (c) of

---

[81] The "permitted maximum" is either 3 or 6 months, depending upon whether the examination of the material is certified as necessary in the interests of national security: see section 16(3A) RIPA.

[82] §6.4 of the Code states:
"A section 8(4) warrant authorises the interception of external communications. Where a section 8(4) warrant results in the acquisition of large volumes of communications, the intercepting agency will ordinarily apply a filtering process to automatically discard communications that are unlikely to be of intelligence value. Authorised persons within the intercepting agency may then apply search criteria to select communications that are likely to be of intelligence value in accordance with the terms of the Secretary of State's certificate. Before a particular communication may be accessed by an authorised person within the intercepting agency, the person must provide an explanation of why it is necessary for one of the reasons set out in the certificate accompanying the warrant issued by the Secretary of State, and why it is proportionate in the particular circumstances. This process is subject to internal audit and external oversight by the Interception of Communications Commissioner. Where the Secretary of State is satisfied that it is necessary, he or she may authorise the selection of communications of an individual who is known to be in the British Islands. In the absence of such an authorisation, an authorised person must not select such communications."

RIPA (*i.e.* in interests of national security, for the purpose of preventing or detecting serious crime or for the purpose of safeguarding the economic well-being of the United Kingdom, in circumstances appearing to the Secretary of State to be relevant to the interests of national security). In other words, the certificate regulates the examination of the intercepted material (see §6.14 of the Code). In addition, any individual selection of intercepted material must be proportionate in the particular circumstances (given s. 6(1) HRA, and see §§3.6-3.7 of the Code). Further, provision is made in s. 16 RIPA to limit the extent to which intercepted material can be selected by reference to "factors" that in essence would select communications to or from an individual who is known to be (at the time) in the British Islands. The Commissioner has confirmed that the s. 8(4) regime does not authorise indiscriminate trawling (see the 2013 Annual Report at §6.5.43 [***See Annex 11***]).

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

2.78 It is thus necessary and important to distinguish between the act of interception in and of itself; and a person actually reading, looking at or listening to intercepted material. That is the distinction which the misleading characterisation of the s.8(4) Regime as entailing "mass surveillance" consistently fails to recognise.

2.79 Further detail of the s.16 arrangements is set out in the Code at §§7.14-7.19:

> *"7.14 In general, automated systems must, where technically possible, be used to effect the selection in accordance with section 16(1) of RIPA. As an exception, a certificate may permit intercepted material to be accessed by a limited number of specifically authorised staff without having been processed or filtered by the automated systems. Such access may only be permitted to the extent necessary to determine whether the material falls within the main categories to be selected under the certificate, or to ensure that the methodology being used remains up to date and effective. Such checking must itself be necessary on the grounds specified in section 5(3) of RIPA. Once those functions have been fulfilled, any copies made of the*

material for those purposes must be destroyed in accordance with section 15(3) of RIPA. Such checking by officials should be kept to an absolute minimum; whenever possible, automated selection techniques should be used instead. Checking will be kept under review by the Interception of Communications Commissioner during his or her inspections.

7.15 Material gathered under a section 8(4) warrant should be read, looked at or listened to only by authorised persons who receive regular mandatory training regarding the provisions of RIPA and specifically the operation of section 16 and the requirements of necessity and proportionality. These requirements and procedures must be set out in internal guidance provided to all authorised persons and the attention of all authorised persons must be specifically directed to the statutory safeguards. All authorised persons must be appropriately vetted (see paragraph 7.10 for further information).

7.16 Prior to an authorised person being able to read, look at or listen to material, a record should be created setting out why access to the material is required consistent with, and pursuant to, section 16 and the applicable certificate, and why such access is proportionate. Save where the material or automated systems are being checked as described in paragraph 7.14, the record must indicate, by reference to specific factors, the material to which access is being sought and systems should, to the extent possible, prevent access to the material unless such a record has been created. The record should include 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 the collateral intrusion. All records must be retained for the purposes of subsequent examination or audit.

7.17 Access to the material as described in paragraph 7.15 must be limited to a defined period of time, although access may be renewed. If access is renewed, the record must be updated with the reason for the renewal. Systems must be in place to ensure that if a request for renewal is not made within that period, then no further access will be granted. When access to the material is no longer sought, the reason for this must also be explained in the record.

7.18 Periodic audits should be carried out to ensure that the requirements set out in

section 16 of RIPA and Chapter 3 of this code are being met. These audits must include checks to ensure that the records requesting access to material to be read, looked at or listened to have been correctly compiled, and specifically, that the material requested falls within the matters certified by the Secretary of State. Any mistakes or procedural deficiencies should be notified to management, and remedial measures undertaken. Any serious deficiencies should be brought to the attention of senior management and any breaches of safeguards (as noted in paragraph 7.1) must be reported to the Interception of Communications Commissioner. All intelligence reports generated by the authorised persons must be subject to a quality control audit.

7.19 In order to meet the requirements of RIPA described in paragraph 6.3 above, where a selection factor refers to an individual known to be for the time being in the British Islands, and has as its purpose or one of its purposes, the identification of material contained in communications sent by or intended for him or her, a submission must be made to the Secretary of State, or to a senior official in an urgent case, giving an explanation of why an amendment to the section 8(4) certificate in relation to such an individual is necessary for a purpose falling within section 5(3) of RIPA and is proportionate in relation to any conduct authorised under section 8(4) of RIPA."

2.80 Although the full details of the s. 16 arrangements cannot be made public (Mr Farr §100), records must be kept of them, and they must be made available to the Commissioner (§§6.28 and 7.1 of the Code[83]), who is required to keep them under review (see s. 57(2)(d)(i) of RIPA). Any breach of the arrangements must be reported to the Commissioner (§7.1 of the Code[84]). Further, if the Commissioner considers that the arrangements have proved inadequate in any relevant respect he must report this to the Prime Minister (see s. 58(3)).

2.81 The Commissioner's advice and approval was sought and given in respect of the documents constituting the s. 16 arrangements either before or shortly after 2 October 2000 (when RIPA came into force): §15 of the Commissioner's Annual Report for 2000 (See Annex 35). In practice, the advice of the Commissioner is sought when any substantive change is proposed to the arrangements.

[83] See also to similar effect §5.17 of the 2002 Code.
[84] See also to similar effect §6.1 of the 2002 Code.

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

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

2.83 A section 8(4) warrant may be renewed at any point before its expiry date. The application for renewal must be made to the Secretary of State, and must contain all the detailed information set out in §6.10 of the Code, just as with the original warrant application (see §6.22 of the Code[85]). The Code states at §6.22 with regard to the renewal application:

> *"…the applicant must give an assessment of the value of interception to date and explain why it is considered that interception continues to be necessary for one or more of the statutory purposes in section 5(3), and why it is considered that interception continues to be proportionate."*

2.84 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: s. 9(2). Further, by s. 9(3), the Secretary of State must cancel a s. 8(4) warrant if he is satisfied that the warrant is no longer necessary on grounds falling within s. 5(3). Detailed provision is made for the modification of warrants and certificates by s. 10 RIPA.

2.85 §6.27 of the Code requires records to be kept of copies of all renewals and modifications of s. 8(4) warrants / certificates, and the dates on which interception is started and stopped (and §5.17 of the 2002 Code was to like effect).

The handling and use of intercepted material and related communications data

[85] See also to parallel effect §5.12 of the 2002 Code.

2.86 Section 15(1)(a) RIPA imposes a duty on the Secretary of State to ensure, in relation to s. 8(4) warrants (and s. 8(1) warrants), that such arrangements are in force as he considers necessary for securing that the requirements of ss. 15(2) and 15(3) are satisfied in relation to the intercepted material and any related communications data.[86] As regards material intercepted under the s. 8(4) regime, the requirements in ss. 15(2) and 15(3) apply both to intercepted material that may be read, looked at or listened to pursuant to s. 16 RIPA and the certificate in question (and s. 6(1) HRA) and to material that may not be so examined. Further, given the definition of "intercepted material", it is clear that ss. 15(2) and 15(3) apply both to external communications and to any internal communications that may also have been intercepted under a s. 8(4) warrant.

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

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

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

2.89 By s. 15(5) RIPA, the s. 15(2) arrangements must include such arrangements as the Secretary of State considers necessary for securing that every copy of the material / data is stored, for so long as it is retained, in a secure manner.[87]

[86] This duty is subject to s. 15(6) (see §2.99 below).
[87] The seventh data protection principle imposes a similar obligation, insofar as the intercepted material amounts to personal data.

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

> *"…each copy of the material or data (if not destroyed earlier) is destroyed as soon as there are no longer any grounds for retaining it as necessary for any of the authorised purposes."*[88]

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

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

2.91 Chapter 7 of the Code expands on the nature of these safeguards. It begins by emphasising at §7.1 that all material intercepted under a s. 8(4) warrant (including related communications data) must be handled in accordance with the safeguards that the Secretary of State has approved under section 15.

2.92 The Code then provides further information about the s. 15 safeguards, including information about safeguards on disclosure to foreign states. As regards the dissemination of intercepted material and any related communications data, §7.3-7.5 provide[89]:

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

[89] See also §§6.4-6.6 of the 2002 Code.

"*7.3 The number of persons to whom any of the intercepted material*[90] *is disclosed, and the extent of disclosure, must be limited to the minimum that is necessary for the authorised purposes set out in section 15(4) of RIPA. This obligation applies equally to disclosure to additional persons within an agency, and to disclosure outside the agency.*[91] *It is enforced by prohibiting disclosure to persons who do not hold the required security clearance, and also by the need-to-know principle: intercepted material must not be disclosed to any person unless that person's duties, which must relate to one of the authorised purposes, are such that he needs to know about the material to carry out those duties.*[92] *In the same way only so much of the material may be disclosed as the recipient needs. For example if a summary of the material will suffice, no more than that should be disclosed.*

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

7.5 Where intercepted material is disclosed to the authorities of a country or territory outside the UK, the agency must take reasonable steps to ensure that the authorities in question 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. In particular, the intercepted material must not be further disclosed to the authorities of a third country or territory unless explicitly agreed with the issuing agency, and must be returned to the issuing agency or securely destroyed when no longer needed."

2.93 Further, as §7.10 of the Code makes clear, arrangements regarding personnel security impose strict limits on who may gain access to intercepted material and any related communications data[93]:

[90] It is apparent from the drafting of §7.1 of the Code that references in Chapter 6 to "the material" and "the intercepted material" are to the material intercepted under an interception warrant, including any related communications data, and that therefore those terms do not bear the technical meaning given to them in s. 20 of RIPA.

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

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

[93] See also to parallel effect §6.9 of the 2002 Code.

> "*All persons who may have access to intercepted material or need to see any reporting in relation to it must be appropriately vetted. On an annual basis, managers must identify any concerns that may lead to the vetting of individual members of staff being reconsidered. The vetting of each individual member of staff must also be periodically reviewed. Where it is necessary for an officer of one agency to disclose intercepted material to another, it is the former's responsibility to ensure that the recipient has the necessary clearance.*"

2.94 The Government's policy on security vetting was announced to Parliament by the then Prime Minister in 1994. The policy was most recently set out in a Cabinet Office booklet, "*HMG Personnel Security Controls*" (***See Annex 36***). In practice, the policy ensures that those who may have access to intercepted material and any related communications data have been rigorously vetted.

2.95 §7.6 of the Code explains the restrictions and safeguards that apply to copying[94]:

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

2.96 The safeguards in relation to storage and destruction are addressed in §§7.7 and 7.8-7.9 of the Code[95] respectively:

> "*7.7 Intercepted material, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of vetting. This*

[94] §6.6 of the 2002 Code was to exactly the same effect.
[95] See also §§6.7-6.8 of the 2002 Code, which contained the same provisions as §§7.7-7.8 of the Code.

requirement to store intercept product securely applies to all those who are responsible for the handling of this material, including [communications service providers]....
material

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

7.9 Where an intercepting agency undertakes interception under a section 8(4) warrant and receives unanalysed intercepted material and related communications data from interception under that warrant, the agency must specify (or must determine on a system by system basis) maximum retention periods for different categories of the data which reflect its nature and intrusiveness. The specified periods should normally be no longer than two years, and should be agreed with the Interception of Communications Commissioner. Data may only be retained for longer than the applicable maximum retention periods if prior authorisation is obtained from a senior official within the particular intercepting agency on the basis that continued retention of the data has been assessed to be necessary and proportionate. If continued retention of any such data is thereafter assessed to no longer meet the tests of necessity and proportionality, it must be deleted. So far as possible, all retention periods should be implemented by a process of automated deletion, which is triggered once the applicable maximum retention period has been reached for the data at issue.[96]*"*

2.97 Although the full details of the s. 15 safeguards cannot be made public [Mr Farr *§100*], they are made available to the Commissioner (§7.1 of the Code[97]) who is required to keep them under review (see s. 57(2)(d)(i) RIPA). Further, to facilitate oversight by the Commissioner, each intercepting agency is required to keep a record of the arrangements for meeting the requirements of sections 15(2) and (3) RIPA (see

[96] §7.9 has been added in the new version of the Code (i.e. the version from January 2016) to reflect the Disclosure in the Liberty proceedings.
[97] And see, to the same effect, §6.1 of the 2002 Code.

§6.28 of the Code). Any breach of the arrangements must be reported to the Commissioner (§7.1 of the Code), and if the Commissioner considers that the arrangements have proved inadequate in any relevant respect he must report this to the Prime Minister (see s. 58(3) RIPA).

2.98 The Commissioner's advice and approval was sought and given in respect of the documents constituting the s. 15 arrangements either before or shortly after 2 October 2000 (when RIPA came into force): §15 of the Commissioner's 2000 Annual Report 2000 [***See Annex 35***]. In practice, the advice of the Commissioner is sought when any substantive change is proposed to the s. 15 arrangements that apply under the s. 8(4) regime [*Farr §104*].

2.99 For completeness, s. 15(6) RIPA is to be noted.

> "*Arrangements in relation to interception warrants which are made for the purposes of subsection (1) –*
>
> *(a) shall not be required to secure that the requirements of subsections (2) and (3) are satisfied in so far as they relate to any of the intercepted material or related communications data, or any copy of any such material or data, possession of which has been surrendered to any authorities of a country or territory outside the United Kingdom; ...*"

Instead, the s. 15(1) arrangements must secure that possession of the intercepted material and data (or copies thereof) is only surrendered to authorities of a country or territory outside the United Kingdom if it appears to the Secretary of State that requirements corresponding to those in ss. 15(2)-(3) will apply, to such extent (if any) as the Secretary of State thinks fit and that, in effect, appropriate restrictions are in place as regards the potential use of any of the intercepted material in proceedings outside the United Kingdom. See s. 15(6)(b) and s. 15(7). As the explanatory notes make clear, ss. 15(6)-(7) apply to the surrendering of communications / communications data pursuant to an <u>obligation</u> under a mutual assistance agreement. They do not apply to the <u>discretionary</u> disclosure of communications / communications data to any foreign intelligence agency under the SSA / ISA as read with s. 19 CTA and s. 6(1) HRA. Such discretionary disclosures have to comply with

the "*arrangements*" required by s. 15(2) and s. 15(3) RIPA.

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

(1) Where an interception warrant has been issued or renewed, s. 19(1) RIPA imposes a duty on, among others, every person holding office under the Crown to keep secret "everything" in the intercepted material, together with any related communications data. Subject to certain limited defences (including the defence under s. 19(9)(b) that the disclosure was confined to a disclosure authorised by the warrant or the person to whom the warrant is or was addressed), it is an offence for a person to make a disclosure to another of anything that he is required to keep secret under s. 19. Any disclosure of intercepted material or related communications data in breach of the s. 15 arrangements would constitute a criminal offence under s. 19 (unless, exceptionally, one of the defences in s. 19 applied). The maximum penalty for this offence is a fine and five years imprisonment. See s. 19(4) RIPA.

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

(3) By s. 8 OSA, it is also an offence for members of the Intelligence Services to fail to take reasonable care to prevent unauthorised disclosure of *e.g.* documents that contain intercepted material (or related communications data). See §§3.22-3.23 above.

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

The practical operation of the s. 8(4) Regime

2.101 In §6.5.1 of his 2012 Annual Report, 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*."

2.102 To similar effect, the Commissioner concluded as follows in his 2013 Annual Report:

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

2.103 In his 2014 Annual Report (***See Annex 12***), the Commissioner indicated that he had undertaken a detailed investigation into GCHQ's [98] 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*

[98] 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.

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.

2.104 The Commissioner also stated at §6.40 of the 2014 Report (***See Annex 12***):

> *"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."*

Oversight mechanisms in the s. 8(4) regime

2.105 There are three principal oversight mechanisms in the s. 8(4) Regime:

(1) the Commissioner (see §§2.106-2.119 below);
(2) the ISC (see §§2.27-2.34 above); and
(3) the IPT (see §§2.35-2.41 above, and §§2.120-2.124 below).

The Commissioner

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

2.107 The Prime Minister is under a duty to appoint a Commissioner (see s. 57(1) RIPA). By s. 57(5), the person so appointed must hold or have held high judicial office, so as to ensure that he is appropriately independent from the Government. The Commissioner was Sir Anthony May from 31 December 2012 until 4 November 2015, when Sir Stanley Burnton was appointed. The Commissioner (quite properly) considers himself to be independent from Government and the Intelligence Services: see e.g. the 2013 Annual Report at §§6.3.1-6.3.4 (***See Annex 11***).

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

> "*…the [Commissioner] shall keep under review-*
>
> *(a) the exercise and performance by the Secretary of State of the powers and duties conferred or imposed on him by or under sections 1 to 11;*
>
> *…*
>
> *(d) the adequacy of the arrangements by virtue of which-*
>
> *(i) the duty which is imposed on the Secretary of State…by section 15*[99]*…*
>
> *[is] sought to be discharged*."

2.109 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).

2.110 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 (2014 Annual Report, §6.51 [***See Annex 12***]). Inspections are thorough and detailed. A typical inspection of an interception agency will include the following (see 2014 Annual Report, §6.46):

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

"- *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."*

2.111 Representative samples of warrantry paperwork are scrutinised (2014 Annual Report §6.52) including the paperwork for s. 8(4) warrants (Farr §91). The total number of warrants specifically examined equated in 2014 to 58% of the extant warrants at the end of the year, and 34% of new warrants issued in 2014 (2014 Annual Report, §6.53). The examination process is a 3-stage one, as the 2014 Report explains at §6.52:

" - *First, to achieve a representative sample of warrants we select from 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…*

- *Second, we scrutinise the selected warrants and associated documentation in detail during reading days which precede the inspections.*
- *Third, 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."*

2.112 The Commissioner also produces 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 (2014 Annual Report at §6.47). The Commissioner meets with the relevant Secretaries of State (2014 Annual Report at *§3.33*).

2.113 In addition to these regular inspections, the Commissioner has power to (and does) 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***).

2.114 S. 58 RIPA imposes important reporting duties on the Commissioner. (It is an indication of the importance attached to this aspect of the Commissioner's functions that reports are made to the Prime Minister.)

2.115 The Commissioner is by s. 58(4) under a duty to make a report every six months[100] to the Prime Minister regarding the carrying out of his functions. Pursuant to s. 58(6), a copy of each six-monthly report (redacted, where necessary, under s. 58(7)) must be 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's practice is to make six-monthly reports in open form, with a closed confidential annex for the benefit of the Prime Minister going into detail on any matters which cannot be discussed openly.

[100] s.58 RIPA was amended with effect from 17 July 2014 to provide for six-monthly reports: previously, reports were annual.

2.116 Further, s. 58 provides:

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

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

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

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

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

2.119 The Commissioner's oversight functions are supported by the record keeping obligations that are imposed as part of the s. 8(4) regime. See §2.85, §2.80 and §2.97 above; and §§6.27-6.28 of the Code. His oversight functions are further supported by the obligation to report any breaches of the ss. 15 and 16 arrangements pursuant to

§7.1 of the Code (see §2.80 above). In practice, all the agencies that are empowered to conduct interception have arrangements in place with the Commissioner to report errors that arise in their interception operations. The Commissioner addresses such errors in his six-monthly reports (see *e.g.* §§3.58-3.68 of the 2013 Annual Report [See Annex 11]).

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

2.120 As regards the s. 8(4) regime, the following specific aspects of the IPT's jurisdiction are of particular relevance. The IPT has exclusive jurisdiction to consider claims under s. 7(1)(a) HRA that relate to conduct for or in connection with the interception of communications in the course of their transmission by means of a telecommunication system:

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

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

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

65(4), 65(5)(b), 65(7)(b) and 65(8)(a) of RIPA).

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

2.123 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.

2.124 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.

3 PART 3 – RESPONSE TO THE GROUNDS

QUESTION 1. THE INTELLIGENCE SHARING REGIME

The Applicants do not have victim status

3.1 The Applicants do not contend, and have put forward no evidential basis for contending, that their communications have in fact been intercepted under the Prism or Upstream programmes, and subsequently shared with the Intelligence Services. Rather, they assert only that they "believe" that this is the case, but no evidential basis is provided for that assertion: see Additional Submissions on the Facts and Complaints at §7. 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.

3.2 The Grand Chamber has recently 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* (app. 47143/06, 4 December 2015). *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.

3.3 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."*

3.4 As to the second condition, 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 avenues for challenge and 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.

3.5 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[101]. 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. Further, as set out below at §§4.17-4.19, those conditions substantially mirror, and are no narrower than, 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, the SSA or ISA. They suggest that their data may be shared with the UK because of their human rights activities. But 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

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

sharing without a warrant in pursuance of the Intelligence Services' statutory functions. The Applicants do not contend otherwise.

3.6 **Secondly**, the Applicants did complain at the national level about whether they might have been subject to unlawful intelligence sharing, but no such determination was made by the IPT. Had there been unlawful sharing of their data, the IPT would have so declared, and would been empowered to make any order it saw fit, including an order for compensation, and the destruction of the data in question (see s.67(7) RIPA). Thus, for example, the IPT would have declared the sharing of the Applicants' data with the Intelligence Services to be unlawful in any of the following circumstances:

(1) Data was shared where a warrant covering the Applicant's communications was in place, but the conditions for the issue of a warrant were not met.
(2) Data was shared where a warrant covering the Applicant's communications was in place, and the conditions for the issue of a warrant were met, but the particular data could not lawfully and proportionately be shared pursuant to the relevant Intelligence Service's statutory functions.
(3) Data was shared where no warrant covering the Applicant's communications was in place, and the Secretary of State had not personally decided that a request for the Applicant's communications should be made.
(4) Data was shared where no warrant covering the Applicant's communications was in place, the Secretary of State had personally decided that a request for the Applicant's communications should be made, but such a request was not lawful and proportionate in pursuance of the Intelligence Services' statutory functions.

3.7 The effectiveness of the IPT in investigating allegations of unlawful intelligence sharing in these circumstances is amply demonstrated by its careful and exhaustive consideration of the relevant legal regime and the treatment of the applicants' own communications in the Liberty proceedings. The fact that the IPT is (and has shown itself to be) an effective domestic route of challenge makes it unnecessary and inappropriate for the Court to entertain an abstract challenge to the Intelligence

Sharing Regime as a whole, brought by Applicants who have failed to put forward a plausible case that their data has been shared pursuant to that regime.

The "in accordance with the law" and "necessity" tests

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

3.8 The expression "in accordance with the law" requires:

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

3.9 The interferences plainly have a *basis in domestic law*. The statutory provisions in the Intelligence Sharing Regime 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 inter alia s.6(1) HRA).

3.10 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[102], contrary to the submissions made at §72(3) of the Applicants' Additional Submissions. 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.)

3.11 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

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

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.

3.12 **First**, the regime is sufficiently clear as regards the circumstances in which the Intelligence Services can in principle **obtain** information from the US authorities, which has been gathered under the Prism or Upstream programmes.

3.13 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 (see above), 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 communications systems[103] - 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. It will be noted that these purposes 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 – see §2.53 above). 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[104]).

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

[104] 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

3.14 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 to be 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:

> *"As to the nature of the offences, the Court emphasises that the condition of foreseeability does not require states to set out exhaustively by name the specific offences which may give rise to interception. However, sufficient detail should be provided of the nature of the offences in question. In the case of RIPA, s.5 provides that interception can only take place where the Secretary of State believes that it is necessary in the interests of national security, for the purposes of preventing or detecting serious crime or for the purposes of safeguarding the economic well-being of the United Kingdom. The applicant criticises the terms "national security" and "serious crime" as being insufficiently clear. The Court disagrees…"*

3.15 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). See too e.g. *Esbester v UK* (app. 18601/91), April 1993, where the Commission found the statutory functions of the Security Service under the SSA to satisfy the demands of foreseeability in the context of security checking. (By contrast, the cases upon which the Applicants rely at §126 of their Application – *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.)

3.16 Moreover, the circumstances in which the Intelligence Services may obtain information under the Intelligence Sharing Regime are further defined and

---

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.

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[105].

(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 (see §2.21 above). 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.

[105] See §48(2) of the IPT's 5 December judgment.

3.17 **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.

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

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

3.20 Further, ss. 1-2 of the SSA and ss. 1-2 and 3-4 of the ISA, as read with ss. 19(3)-(5) of the CTA and s. 6(1) of the HRA, sufficiently address the circumstances in which the

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

3.21 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.

3.22 **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. The relevance of oversight mechanisms in the assessment of foreseeability, and in particular the existence of adequate safeguards against abuse, is well established in the Court's case law: see e.g. *Kennedy*: when considering the general ECHR-compatibility of the RIPA s. 8(1) regime, the Court at §§155-170 of *Kennedy* "*jointly*" considered the "*in accordance with the law*" and "*necessity*" requirements, and in particular analysed the available oversight mechanisms (at §§165-168) in tandem with considering the foreseeability of various elements of the regime (§§156-164). See too the Grand Chamber's judgment in *Zakharov*, where the Court examined *"with particular attention"* the supervision arrangements provided by Russian law, as part of its assessment of the existence of adequate safeguards against abuse: §§271-280.

3.23 The statutory oversight mechanisms of the ISC and IPT are important and effective, and the Applicants' criticisms of them in their Application and Update Submissions are misplaced.

3.24 As concerns the *ISC*:

(1) The ISC sets its own agenda and work programme and provides an effective strand of the relevant oversight (see Farr §70 and Domestic Law and Practice above).

(2) Indeed, it proactively determined to address allegations both about the alleged Tempora operation and about intelligence sharing in the context of Prism, and has done so in very considerable detail, with the benefit of evidence from many interested parties in its Statement of 17 July 2013 and the ISC Report. The Report addresses the activities of all the Intelligence Services; and was written with the benefit of 56 substantive submissions from parties including privacy advocates, NGOs and the media, and after a number of public evidence sessions, taking evidence from "*both sides of the debate*": see ISC Report, §14[106].

(3) It may be noted that in the Statement of 17 July 2013 the ISC expressed itself satisfied that it had received full information about "*the whole range of Agency capabilities, how they are used and how they are authorised*": see ISC Report, §12. That reflects the obligation on the Heads of the Intelligence Services to arrange for any information requested by the ISC in the exercise of its functions to be made available to it (see Mr Farr, *§67*).

3.25 The *IPT* has broad jurisdiction and extensive powers (including to require the Intelligence Services to provide it with all relevant information to determine complaints). Any person may bring a claim in the IPT: and they need not be able to adduce any evidence that the Intelligence Services have engaged in relevant "conduct" in relation to them, in order to have their complaint considered and determined. The governing provisions have been dealt with above. Its rigorous and detailed judgments in the domestic proceedings plainly indicates that it provides an effective safeguard against abuse.

3.26 The *Commissioner* also offers an effective mechanism for overseeing the internal arrangements under s.15 RIPA. The fact that those same arrangements are *de facto* subject to oversight by the Commissioner in the context of material obtained under the Intelligence Sharing Regime is yet another safeguard against abuse.

3.27 The Court should also take into account in the foreseeability test, just as it did in *Kennedy* at §168, the fact that the investigations by the oversight bodies have not revealed any deliberate abuse by the Intelligence Services of their powers. Neither

[106] ***[See Annex 13]***

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 investigated this allegation - see in particular:

(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[107];

(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[108]).

3.28 **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[109], 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.

Specific points made in the Applicants' Additional Submissions on the Facts and Complaints

3.29 The Applicants assert that the IPT's approach to the intelligence sharing regime was based on a "fundamental error" because they say that the IPT wrongly applied a "significantly attenuated" version of the *Weber* criteria (i.e. the six "minimum

[107] See ***[Annex 21]***. The investigation that preceded the ISC's Statement was thorough. See §5 of the Statement.

[108] [***See Annex 11]***

[109] 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."

safeguards" to which the Court referred at §95 of *Weber*[110]) (see §71 of the Applicants' Additional Submissions). That argument is unsustainable. 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.

3.30 *Weber* concerns interception **by the respondent State**. The Applicants do not cite <u>any</u> Art. 8 case that concerns a complaint that the intelligence agencies of the respondent State had 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 Government are aware, the application of Art. 8 to cases of this latter type has never been considered by the Court.

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

3.32 **First**, the 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: *Uzun v. Germany* at §66. The Court has never suggested that this form of wide-ranging and detailed statutory 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*").

3.33 **Secondly,** the 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

---

110 "*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).

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.

3.34 **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 non-intercept communications/communications data, intelligence from covert human intelligence sources (as they would be termed under RIPA) or covert audio / visual surveillance. In many contexts, the Intelligence Services may not even know whether communications or communications data provided to them by a foreign intelligence agency have been obtained as a result of interception. 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 (Mr Farr §§27-30). 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.

3.35 If the *Weber* criteria apply to the obtaining of intercept material from a foreign intelligence agency, and if the Intelligence Sharing Regime does not satisfy those criteria, then it is difficult to see how the Intelligence Services could lawfully obtain <u>any</u> information from a foreign intelligence agency about an individual that derived from covert human intelligence sources, covert audio / visual surveillance or covert property searches. But that would be a remarkable, and deeply concerning, conclusion - not least given that intelligence sharing is (and has for many years been) vital to the effective operation of the Intelligence Services (see Mr Farr *§§15-26*).

3.36 **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) all 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 the reasons already set out at §4.102 above, and expanded upon by Mr Farr at §§56-61.

3.37 **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 §§3.8-3.28 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 §§3.12-3.16 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);
(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).

3.38 In terms of the Applicants' reasons for suggesting that the Intelligence Sharing Regime is "not in accordance with the law" (see §72 of the Applicants' Additional Submissions), the Government repeats §§3.8-3.28 above. The Code itself is "law" for the purposes of the "in accordance with the law" test: see e.g. *Kennedy*. So, to the extent that the Intelligence Services' internal arrangements are set out in the Code, they are indeed "law". Moreover, the Disclosure is also "law" for these purposes: it is a published statement, contained in publicly accessible court judgments: see §3.10 above.

3.39 There is a very good reason why the Code summarises certain important aspects of the internal arrangements, rather than setting them out in full. To set them out in full would have the effects set out by Mr Farr at §§55-61, and correspondingly undermine the interests of national security. It would reveal existing intelligence relationships; show hostile individuals what sort of information is shared, and how; damage relations with intelligence partners; reduce the quality of and quantity of intelligence available to the Intelligence Services; limit operational flexibility; and risk offering additional insights into the activities of the Intelligence Services whenever they were revised. Further, the IPT agrees. It investigated the internal arrangements, and found that further disclosure would risk damaging national security and the NCND principle (see the 5 December Judgment, §50(iv)).

3.40 Moreover, even if unpublished arrangements are not themselves "law", they are plainly relevant both to the foreseeability of the Intelligence Sharing Regime and the fulfilment of the underlying purpose for which the "in accordance with law" requirement exists in this context, namely to protect against arbitrary or abusive conduct by the State. The fact that further internal arrangements are known to exist, have been assessed by the IPT, and are subject to oversight as set out above is itself a relevant safeguard against abuse: see above.

The "necessity" test

3.41 The Applicants rightly make no submissions on the "necessity" of the Intelligence Sharing Regime. No separate question of "necessity" arises with regard to the Intelligence Sharing Regime, 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[111]. To that

[111] 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.

end it is pertinent that the Applicants' individual allegations of unlawful intelligence sharing were not upheld in the domestic IPT proceedings.

4 QUESTION 2. THE SECTION 8(4) REGIME

Victim status

4.1 The conditions under which an applicant can claim to be a victim of secret surveillance measures violating Article 8 ECHR have been addressed in detail above at §§3.2-3.4 in the context of the Intelligence Sharing Regime, with particular reference to the Grand Chamber decision in *Zakharov*. In the context of the s.8(4) Regime and on the basis of the assumed facts at §§1.26-1.28 and §§2.77-2.78 above, the key stage is evidently the selection and examination stage i.e. the point at which a person actually reads, looks at, or listens to intercepted material. Therefore, in this context (and as with the Intelligence Sharing Regime), a person needs to be able to demonstrate that they are at realistic risk of selection/examination which means being able to demonstrate that they have reason to believe their communications are of interest to the Intelligence Services on the grounds mentioned in s.5(3)(a), (b) or (c) (i.e. in the interests of national security, for the purposes of preventing or detecting serious crime or for the purpose of safeguarding the economic well-being of the United Kingdom); grounds which mirror the statutory functions of the Intelligence Services. Unless those grounds are satisfied then any selection and examination would be unlawful. For the reasons set out at §3.5(4) above, none of the Applicants can satisfy that test (save in this s.8(4) context for the Legal Resources Centre and Amnesty International, given the IPT's conclusions in the 22 June 2015 judgment (see §1.50 above)).

The "in accordance with law" and "necessity" tests

4.2 Before addressing the application of the "in accordance with the law" and "necessity" tests under Article 8 ECHR in detail, five preliminary points should be noted at the outset:

i. Some form of s. 8(4) Regime is a practical necessity.
ii. The s. 8(4) Regime was designed on this basis, and with the internet in mind.
iii. The existing ECtHR interception case law - and in particular *Weber*, *Liberty* and *Kennedy* - supports the Government's position that the "*in accordance with the law*" requirement is satisfied.
iv. By contrast, *Digital Rights Ireland* is not relevant to this issue.
v. 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.

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

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

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

4.5 The fact is that the Government has no choice in this regard if it is to obtain the external communications it considers necessary for safeguarding the UK's national security. The reasons why that is the case follow from the summary of the facts at §§1.29-1.35 above. As the Commissioner has confirmed, following an "*in detail*" investigation of the relevant (and sensitive) technical background relating to the procedure under the s. 8(4) Regime, *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.

4.6 It is for these reasons that the Intelligence Services intercept the entirety of the contents of a bearer or bearers, and then subject them to an automated filtering process (resulting in much of the intercepted material being immediately discarded) in order to obtain any of the communications in which they are interested, while they transit the internet. The only practical way to find and reconstruct most external communication "needles" is to look through the communications "haystack".

4.7 So unless it is said that the Intelligence Services should not be able to obtain the external communications that they need to protect the UK's national security, the Applicants must accept *some* form of interception regime that permits substantially more communications to be intercepted (including, potentially, internal communications) than are actually being sought. Or, to continue the analogy in the paragraph above, they must accept a regime that permits the acquisition of "haystacks" in order to find communications "needles".

4.8 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 Mr Farr §§142-147. Those practical differences offer further justification for a regime of the form of the s. 8(4) Regime (Mr Farr §149): see §1.32 above.

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

4.9 The s. 8(4) regime was - to Parliament's knowledge – designed to accommodate the internet, and Parliament was made aware of the issue just noted: see Lord Bassam in Lords Committee (Hansard, 12 July 2000 at column 323[112]):

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

4.10 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[113]. The fact that there the internet has grown in scale does not render the safeguards under RIPA less relevant or adequate.

iii. *Weber*, *Liberty* and *Kennedy* support the Government's position

4.11 *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

---

112 [***See Annex 26***]

113[***See Annex 11***]

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% 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.

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

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

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

This is unsurprising, not least given the points about the practical necessity of the s.8(4) Regime already made above.

4.13 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). In particular, the ECtHR alluded to the type of details that the German authorities considered it safe to publish about the operation of the G10 Act, under consideration in *Weber;* and noted in this regard that the Code under RIPA (that had been published by the time of the ECtHR's judgment) showed that "*it is possible for a State to make public certain details about the operation of a scheme of external surveillance without compromising national security.*" (§68, emphasis added.)

(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.

4.14 The Applicants are thus plainly wrong to assert that the position remains the same as in *Liberty* and that the IPT misinterpreted the decision in *Liberty*[114]. On the contrary, there is an entirely new statutory regime in place, together with a Code which contains a large number of significant safeguards that were absent from the regime under consideration in *Liberty;* which are directly material to the protection of individuals whose communications may be intercepted pursuant to a s.8(4) warrant; and which the Applicants ignore.

4.15 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.

4.16 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

[114] See Applicants' Additional Submissions at §§49-54.

identical. 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.

iv. *Digital Rights Ireland* is irrelevant

4.17 The Applicants place some reliance upon the judgment of the CJEU in *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and others C-293/12,* 2014/C 175/07, 8 April 2014[115] (See Annex 16). On a proper analysis, the *Digital Rights Ireland* judgment does not affect the approach or conclusions set out above at all. That analysis is supported by the Court of Appeal's reasoning in *R(Davis and Watson) v Secretary of State for the Home Department* [2016] 1 CMLR 48 (See Annex 17).

4.18 *Digital Rights Ireland* was a preliminary reference concerning the validity of Directive 2006/24/EC on Data Retention (See Annex 48), and EU-wide harmonisation measure adopted pursuant to Article 95 EC. The Directive sought to harmonise divergent data retention measures adopted by the Member States under Article 15(1) of Directive 2002/58/EC (See Annex 49)following the terrorist attacks of 11 September 2001 in New York, 11 March 2004 in Madrid, and 7 July 2005 in London. It did this by requiring CSPs in the EU to retain <u>all</u> 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.

4.19 As the CJEU had already made clear in its judgment in *Ireland v European Parliament and Council C-301/06*[116], the provisions of Directive 2006/24/EC were "*essentially limited to the activities of service providers*" and did not "*govern access to data or the use*

[115] See the Additional Submissions on the Facts and the Law at §§66-67.
[116] [***See Annex 50***]

thereof by the police or judicial authorities of the Member States"[117]. Directive 2006/24/EC, as a pre-Lisbon Treaty instrument with its legal base in Article 95 EC, concerning the harmonisation of internal market measures[118], could not include substantive rules relating to access to, or use of, data by national law enforcement authorities.

4.20 In its judgment in *Digital Rights Ireland* concerning the validity of that Directive, the CJEU was therefore not concerned with a national regime or any provision governing access to, or use of, retained data by national law enforcement authorities. The issue before the CJEU was that identified by the Advocate General, namely: *"whether the European Union may lay down a measure such as the obligation to collect and retain, over the long term, the data at issue without at the same time regulating it with guarantees on the conditions to which access and use of those data are to be subject, at least in the form of principles…"*[119]

4.21 In answering that question, the CJEU concluded that the EU legislature was not entitled to adopt the wholesale retention regime laid down in Directive 2006/24/EC without including any safeguards in relation to conditions for access. The CJEU went on to find that Directive 2006/24/EC did not contain any such guarantees, in light of the matters set out at §§56-68 of the judgment[120], and that, by adopting the Directive,

[117] See §§80-82 of the judgment.

[118] Article 95(1) EC provided that "*the Council is to adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market".*

[119] See the Opinion of Advocate General Cruz Villalon, *Digital Rights Ireland,* §121. See also §54 of the CJEU's judgment.

[120] The CJEU made observations at §§56-68 in relation to the following matters:

(1) The broad scope of the data retention envisaged under the Directive (§§56-59);
(2) The absence of any provisions in the Directive defining the limits on access to, and subsequent use of, retained data by national authorities, and in particular the absence of any requirement that access to retained data be dependent on a prior review carried out by a court or independent administrative body (§§60-62);
(3) The length of the data retention period provided for under the Directive, and the absence of any statement that the period of retention had to be based on objective criteria (§§63-64);
(4) The absence of specific rules adapted to the quantity of data whose retention was required, the sensitivity of the data, and the risk of unlawful access to those data; and the absence of any obligation on Member States to establish such rules (§66);
(5) The failure to ensure that a particularly high level of protection and security was applied by service providers, in particular by permitting service providers to have regard to economic considerations when determining the level of security and by failing to ensure the irreversible destruction of the data at the end of the retention period (§67);
(6) The lack of any requirement that data be retained within the EU, with the result that oversight by an independent authority of compliance with the requirements of protection and security could not be fully ensured (§68).

the EU legislature had exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the EU Charter[121].

4.22 The CJEU cannot have intended at §§56-68 of the judgment to lay down a definitive set of requirements that must be incorporated into any data retention regime (still less, access regime) adopted by any Member State of the EU, no matter what other checks, balances or safeguards it already has. On a proper analysis, the *Digital Rights Ireland* judgment does not lay down any minimum requirements for access to or retention of data, nor purports to depart from established principles of ECtHR case law.

4.23 **First**, the case was solely concerned with the validity of Directive 2006/24/EC, which, as the CJEU had already established in *Ireland v Parliament,* did not regulate the activities of national law enforcement authorities. The CJEU had no evidence on which to reach a view about the proportionality of the specific safeguards adopted by any individual Member State to protect personal data against the risk of unlawful access, and did not consider the extent to which matters concerning access to data by national policing or security bodies (and safeguards in relation to such matters) were not subject to EU law. So, in identifying at §§56-68 the type of safeguards that were absent from the EU regime, the CJEU was plainly not deciding that those specific safeguards must, as a matter of EU law, be included in any national data retention or access regime.

4.24 **Secondly**, the judgment does not lay down mandatory requirements for access to or retention of data. EU law does not regulate the ability of national police forces or other law enforcement bodies to access or use personal data (save in the very specific context of EU cross-border cooperation in criminal matters[122]). If the CJEU's judgment were to be read as laying down mandatory requirements for national data

[121] Articles 7, 8 and 52(1) of the Charter provide, as far as material:
"7. Everyone has the right to respect for his or her private and family life, home and communications.
8. (1) Everyone has the right to the protection of personal data concerning him or her…
52 (1) Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may only be made if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."
[122] See Council Framework Decision 2008/977/JHA.

access, it would involve the CJEU legislating in relation to national rules, where such rules are not implementing EU law and where there is no EU law basis for imposing such requirements; and moreover doing so in any area where the EU Treaties specifically recognise the Member States' essential interests and responsibilities[123].

4.25 **Thirdly**, the CJEU has repeatedly confirmed that Article 7 of the Charter must be given the same meaning and scope as Article 8(1) ECHR, as interpreted by the ECtHR[124]. Indeed, where a Charter right corresponds to a right guaranteed by the ECHR, as Articles 7 and 8 both do (data protection being an inherent aspect of the right to respect for private life), Article 52(3) of the Charter requires that the meaning and scope of the rights under the ECHR and the Charter be the same.

4.26 If the CJEU had intended §§56-68 of its judgment to represent a definitive set of requirements for national access/retention regimes, irrespective of what safeguards and access conditions they already contain, that would have represented a clear and radical departure from the principles established by the ECtHR under Article 8 ECHR, as set out below at §§4.32-4.38.

4.27 However, nothing in the CJEU's judgment indicates that it intended to go beyond, expand, or in any way qualify the established principles in the ECtHR's case law on Article 8 ECHR in its application of the Charter. On the contrary, both the Advocate General and the CJEU referred to, and purported to apply, the ECtHR's case law on Article 8 ECHR: see the judgment at §§35, 47, 54, 55. Indeed, the Advocate General expressly referred to the need to "*remain faithful to the approach of the case-law of the European Court of Human Rights*"[125]

4.28 The Court of Appeal in *Davis and Watson*[126] has recently addressed whether the CJEU intended in *Digital Rights Ireland* to lay down definitive mandatory requirements for national regimes concerning the retention of communications data. Mr Davis and Mr

[123] See in particular Article 4(2) of the Treaty on the European Union, which requires the EU to respect Member States' essential State functions, including ensuring territorial integrity, maintaining law and order, and safeguarding national security, the latter of which remains the sole responsibility of each Member State.
[124] See e.g. *McB v Ireland C-400/10* at §53
[125] See the Advocate-General's Opinion at §110.
[126] See [***Annex 17]***

Watson (Members of the UK Parliament) challenged the legality of the Data Retention and Investigatory Powers Act 2014 ("DRIPA"), an Act of Parliament providing for the retention of communications data by communications providers, pursuant to a retention notice served by the Secretary of State. They asserted that DRIPA was inconsistent with EU data protection law on the basis of *Digital Rights Ireland,* which (they said) laid down mandatory requirements for a national retention regime. The Court of Appeal reached the provisional conclusion at §106 of the judgment – essentially, on the basis of the matters set out above – that *Digital Rights Ireland* did not lay down such mandatory requirements, but was concerned simply with the validity of Directive 2006/24/EC. However, the Court of Appeal referred the issue to the CJEU on the basis that it was not *acte clair*. So the CJEU will shortly be reconsidering the effect of its conclusions in *Digital Rights Ireland*.

v. Intercepting communications is in general more intrusive than obtaining communications data

4.29 The Court 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.

4.30 The Claimants appear to dispute this, in particular by reference to the possibility of aggregating communications data eg. to build databases or 'datasets'. 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.

4.31 Nevertheless, it is possible that aggregating communications data may in certain circumstances (and, potentially, with the addition of further information that is not

communications data) 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.

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

4.32 The Art. 8 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[127] 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.

4.33 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*.)

4.34 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

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

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 (see §§4.57-4.64 above).

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

4.35 Subject to the principle set out in §4.33 above, there needs to be clear, detailed rules on the interception of communications to guard against the risk that such secret powers might be exercised arbitrarily (*Weber*, at §§93-94). As has already been noted, the ECtHR has developed the following set of six "*minimum safeguards*" that need to be set out in the domestic legal framework that governs the interception of communications, in order to ensure that the "*foreseeability*" requirement is met in this specific context:

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

4.36 As already noted, *Liberty, Kennedy* and *Zakharov* make clear that it is not necessary that every provision / rule be set out in primary legislation: see §3.33 above.

4.37 §95 of *Weber* applies insofar as the s. 8(4) Regime authorises the interception of communications. First, *Weber* concerned the German equivalent of the s. 8(4) Regime. Secondly, §95 of *Weber* was applied in *Liberty*, which concerned the statutory predecessor to the s. 8(4) Regime. In the light of the above, the various safeguards listed in §95 of *Weber* are addressed - in turn - at §§4.40-4.55 below. Such a point-by-point analysis is a necessary part of determining compliance with the "*in accordance with the law*" requirement for interception: see *e.g.* the ECtHR's approach in §§159-164 of *Kennedy*, and *Weber* itself, at §§96-100. By contrast:

(1) The test is not whether, in one or more respects, the s. 8(4) Regime is somehow broader or less tightly defined then the German strategic monitoring regime at issue in *Weber* (not least because strategic monitoring satisfied the "*in accordance with the law*" requirement by some margin, in that the Art. 8 complaint in *Weber* was thrown out as "*manifestly ill-founded*": §138).
(2) Nor is the test whether the Government might be able to publish some more details of the s. 8(4) Regime or impose at least some more constraints on the powers that are exercised under it.

4.38 As the ECtHR recognised in §95 of *Weber*, the reason why such safeguards need to be in a form accessible to the public is in order to avoid "*abuses of power*". This requirement is thus a facet of the more general principle that there must be adequate and effective guarantees against abuse. Accordingly, in determining whether the domestic safeguards meet the minimum standards set out in §95 of *Weber*, account should be taken of all the relevant circumstances, including: "*the authorities competent to ... supervise [the measures in question], and the kind of remedy provided by the national law ...*" (*Association for European Integration and Human Rights v. Bulgaria*, Appl. no. 62540/00, 28 June 2007, at §77.)

4.39 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. The Government emphasises the following points:

(1) The Commissioner has himself stated that his investigations are "*thorough and penetrating*" and that he has "*no hesitation in challenging the public authorities wherever this has been necessary*" (2013 Annual Report at §6.3.3[128]). As to his powers to compel disclosure / the provision of documents and information, the Commissioner has found "*that everyone does this without inhibition*" and that he is thus "*fully informed, or able to make [himself] fully informed about all interception ... activities ... however sensitive these may be*" (2013 Annual Report at §2.14).[129]
(2) The Commissioner regularly inspects the Intelligence Services and the work

[128] See ***[Annex 11]***
[129] See also §§6.1.1-6.1.2 of the Commissioner's 2013 Annual Report.

of senior officials and staff at the relevant Departments of State, and produces "*detailed*" written reports and recommendations (Mr Farr §§87-95). He also is empowered to investigate individual matters of concern, should he consider it appropriate to do so (see Sections 5-6 of the 2013 Annual Report[130]).

(3) Whilst the full details of the ss. 15 and 16 safeguards cannot safely be put into the public domain (Farr §100), (i) the Commissioner is required to keep them under review (s. 57(2)(d)(i) of RIPA), (ii) any breach of them must be reported to him (§7.1 of the Code) and (iii) in practice his advice is sought when any substantive change is proposed (Mr Farr §104).

(4) The ISC has given detailed and penetrating consideration to the s.8(4) Regime in the ISC Report.

(5) As regards the Tribunal, a claimant does not need to be able to adduce cogent evidence that some steps have in fact been taken by the Intelligence Services in relation to him before his claim will be investigated. As a result of that test, the applicants were able to challenge the s.8(4) Regime in the Liberty proceedings, and the Tribunal fully investigated the regime in those proceedings.

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

4.40 This requirement is satisfied by s. 5 of RIPA, as read with the relevant definitions in s.81 of RIPA and §§6.11-6.12 of the Code. This follows, in particular, from a straightforward application of §159 of *Kennedy*, and §133 of *RE v United Kingdom*. (See further below at §§4.77-4.81 as regards the meaning of "national security").

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

4.41 As is clear from §97 of *Weber*, this second requirement in §95 of *Weber* applies <u>both</u> 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).

[130] See ***[Annex 11]***

4.42 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. The term "external communication" is sufficiently defined in s. 20 and §5.1 of the Code (see §§4.66-4.76 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 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"[131]. Similarly, during the Parliamentary debate on the Bill that was to become RIPA, Lord Bassam referred to intercepting the whole of a communications "link" (see §1.37 above).

(4) In addition, a s. 8(4) warrant may in principle authorise the interception of internal communications insofar as that is necessary in order to intercept the external communications to which the s. 8(4) warrant relates. See s. 5(6) of RIPA, and the reference back to s. 5(6) in s. 8(5)(b) of RIPA (which latter provision needs to be read with s. 8(4)(a) of RIPA). This point was also made clear to Parliament (see §1.37 above) and it has in any event been publicly confirmed by the Commissioner (see §1.39 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*" (see §4.33 above) and in the light of the available oversight mechanisms (see §§2.105-2.124 above), the s. 8(4) regime sufficiently identifies the categories of people who are liable to have their communications intercepted.

[131] See the 5 December Judgment at §93. See too, for example, the ISC Report.

4.43 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.

(2) As regards the former, 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* (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 §§4.77-4.81 below as regards the meaning of "national security".

(3) 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 listened to according to a factor which is (a) referable to an individual who is known to be for the time being in the British Islands and (b) which has as its purpose, or one of its purposes, the identification of material contained in communications sent by him or intended for him.

(4) As found by the IPT "referable to" (s. 16(2)(a)) is a wide term and generally accepted to be so as a matter of statutory construction. It would prohibit the use of terms which were connected with, or could lead to the identity of, the individual by the use of names, nicknames, addresses, descriptions or other similar methods (see §104 of the 5 December judgment in the *Privacy* proceedings). If the term was any more specific then it would become unworkable. In those circumstances the criticisms of this term at §46(3)(a) of the Applicants' Additional Submissions are misplaced).

(5) 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"[132].

(6) As to the suggestion that the term "*known to be* for the time being in the British Islands" (s. 16(2)(a)) does not prevent inspection where there is a "strong suspicion" that the person is in the UK (see §46(3)(b) of the Applicants' Additional Submissions), the latter would clearly pose too high a hurdle, particularly in the course of extended examination of substantial numbers of communications, as found by the IPT at §104 of the 5 December judgment in the *Privacy* proceedings

(7) In addition, the condition at s. 16(2)(b) is not too limited a restriction[133] in circumstances where the aim is to prevent access to communications sent by or sent to an individual who is in the United Kingdom; see the final sentence of §104 of the 5 December judgment in the *Privacy* proceedings.

4.44 The applicants contend that the safeguards in s.16(2) can be "swept aside" by the "wide discretion" given to the Secretary of State under s.16(3) (which provides for strictly limited circumstances in which it is permissible to select intercepted material by reference to factors which satisfy ss. 16(2)(a) and 16(2)(b) – see §2.74 above). That is wrong. The Secretary of State's power to modify a certificate under s. 16(3) so that intercepted material can be selected according to a factor that is referable to a particular identified individual is in substance as tightly constrained as his power to issue a s. 8(1) warrant, the ECHR-compatibility of which was confirmed by the ECtHR in *Kennedy*.

4.45 In addition, it is well established as a matter of domestic law that an authority must discharge its functions so as to promote – and not so as to thwart or act contrary to – the policy and objects of the legislation conferring the powers in question (see *Padfield v Minister of Agriculture Fisheries and Food* [1968] AC 997 and in particular the speech of Lord Reid at p.1030B-D, p.1033A, and p.1045G). Hence it is wrong to

[132] See the Code, §6.14. In addition guidance is given as to how the Secretary of State will assess such necessity: See §7.19 of the Code.

[133] Contrary to the submissions made at 46(3)(c) of the Applicants' Additional Submissions.

suggest [134] that the Intelligence Services could deliberately circumvent the requirements of s.16(2) by taking action where a person was living in the UK but was known to be out of the UK for a short period. That would be to deliberately undermine the policy objectives of the legislation and would be unlawful as a matter of domestic public law.

4.46 These 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.

4.47 The regime thus does not permit indiscriminate trawling, as the Commissioner has publicly confirmed (see his 2013 Annual Report at §6.5.43).

4.48 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.

(3) Limits on the duration of 'telephone tapping'

4.49 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 §§2.82-2.85 above, §161 of *Kennedy*, and the specific provisions for renewal of a warrant contained in §§6.22-6.24 of the Code[135].

[134] See §46(5) of the Applicants' Additional Submissions.

[135] 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

4.50 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.

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

4.51 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).

4.52 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 §§2.69-2.81 above) 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, before any material can be examined at all, the person examining it 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 Code, §§7.14-7.16.

---

the Application, which wrongly states that chapter 6 of the Code does not *"impose any limits on the scope or duration of warrants".*

(2) The Code affords further protections to material examined under the s.8(4) Regime at §§7.11-7.20 (see §§2.79 above). Thus, material should only be examined 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) sets out the precautions to be taken when communicating intercepted material that can be read, looked at or listened to pursuant to s. 16 to other persons (including foreign intelligence agencies: see §3.109 above). 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 (see §2.92 above). 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.

4.53 As already noted, the detail of the s. 15 and s.16 arrangements is kept under review by the Commissioner (see §§2.80-2.81 and §§2.97-2.98 above).

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

4.54 Section 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: see §2.16 above.

4.55 Further there is no merit in the criticism at §47 of the Applicants' Additional Submissions that the destruction provisions in s.15(3) are undermined by the requirement in s.15(4) to retain material where that is necessary for the authorised purposes. The extreme scenario posited in §47 of the Applicants' submissions i.e. a database or dataset where vast quantities of communications and communications data are retained indefinitely, would be contrary to the maximum retention periods spelt out at §7.9 of the Code and would clearly fail to satisfy the requirements of necessity and proportionality if, exceptionally, data is to be held for longer than those periods (see §7.9 of the Code).

Conclusion as regards the interception of communications

4.56 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.

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

Regime

4.57 *Weber* concerned the interception of the content of communications as opposed to the acquisition of communications data as part of an interception operation (see §93 of *Weber*). So far as the Respondents are aware, the list of safeguards in §95 of *Weber* (or similar lists in the other recent ECtHR interception cases) 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.

4.58 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[136]. 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.

4.59 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

[136] See *Uzun* at §66:
"While the Court is not barred from gaining inspiration from [the Weber criteria], it finds that these rather strict standards, set up and applied in the specific context of surveillance of telecommunications, are not applicable as such to cases such as the present one, concerning surveillance via GPS of movements in public places and thus a measure which must be considered to interfere less with the private life of the person concerned than the interception of his or her telephone conversations. It will therefore apply the more general principles on adequate protection against arbitrary interference with art.8 rights as summarised above."

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*).

4.60 The s. 8(4) Regime satisfies this test as regards the obtaining 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[137]. 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 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, if a processing system was able to extract or generate a structured index of the contents of a communication, it would be "metadata"; but would be content for

---

[137] 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."*

the purposes of the s.8(4) Regime. Extracting 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 §§4.41-4.43 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 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.

(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. 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).

4.61 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 (see the Applicants' complaints at §46(1) of their Additional Submissions):

(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)). 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*".

4.62 The regime equally contains sufficient clear provision regarding the subsequent **handling, use and possible onward disclosure** by the Intelligence Services of related communications data. See, *mutatis mutandis*, §§2.86-3.42 above.

4.63 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 §§4.40-4.55 above (and, as regards the limits on the duration of s. 8(4) warrants, §§4.49-4.50 above).

4.64 For the reasons set out above, the s.8(4) Regime is sufficiently foreseeable to satisfy the "in accordance with the law" test, both as regards the interception and handling of the content of communications, and as regards the interception and handling of related communications data.

Further issues regarding foreseeability/accessibility

4.65 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 clarity in the definition of "external communications"[138];
(2) The breadth of the concepts of "national security" and "serious crime" [139].

The definition of "external communications"

4.66 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:

> "*External communications are defined by RIPA to be those which are sent or received outside the British Islands. They include those which are both sent and received outside the British Islands, whether or not they pass through the British Islands in course of their transmission. They do not include communications both sent and received in the British Islands, even if they pass outside the British Islands en route. For example, an email from a person in London to a person in Birmingham will be an internal, not an external, communication for the purposes of section 20 of RIPA, whether or not it is routed via IP addresses outside the British Islands, because both the sender and intended recipient are within the British Islands.*"

4.67 The Applicants complain at §45 of their Additional Submissions about the lack of any practical distinction between internal and external communications and the lack of clarity in relation to external communications. These complaints are unfounded; (and identical complaints were rejected by the IPT in the Liberty proceedings – see 5 December Judgment, §§93-101):

(1) The definition of an "external communication" is sufficiently clear in the

[138] See Additional Submissions at §45.
[139] See Additional Submissions at §46(2).

circumstances.

(2) Whilst in practice the analysis of whether an individual electronic communication is "internal" or "external" may be a difficult one (which can be conducted only with the benefit of hindsight), this has no bearing upon whether a specific communication is likely to be intercepted under the s. 8(4) Regime. The distinction between "external" and "internal" communications is an important safeguard at a "macro" level (when the Intelligence Services decide which communications bearer to intercept): but that exercise has nothing to do with whether a particular communication is "internal" or "external", applying the definition in s.20 RIPA.

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

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

4.68 **First**, the definition of "external communications" is itself a sufficiently clear one, in the circumstances. It draws a distinction between communications that are both sent and received within the British Islands, and communications that are not both sent and received within the British Islands; and the focus of the definition is upon the ultimate sender, and ultimate intended recipient, of the communication. Thus, for the purposes of determining whether a communication is internal or external it matters not that a particular communication may be handled either by persons or by servers en route, who are located outside the British Islands; what matters is only where the sender and intended recipient of the communication are based: see Mr Farr §§129-130. This position reflects what was stated by Lord Bassam during the passage of RIPA through Parliament (set out at §1.37 above).

4.69 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. Thus, where the ultimate recipient is *e.g.* a Google web server (in the case of a Google search), the status of the search query - as a communication - will depend on the

location of the server. Further, when a communication in the form of public post or other public message is placed on a web-based platform such as Facebook or Twitter, the communication will be external if the server in question (as the ultimate recipient) is outside the British Islands. By contrast, if such a platform is used to send what is in effect a private message to a particular individual recipient, then - as in the case of a telephone call, or an ordinary email - the status of the communication in question will depend on whether that recipient is within or outside the British Islands. (And the same analysis applies if the private message is sent to a group of individual recipients: as in the case of an ordinary email, the private message will be an internal communication if all recipients are within the British Islands): see Mr Farr §§133-137.[140]

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

[140] 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 §45(2) of the Additional Submissions, that the Code of Practice is *"silent on the status of many forms of modern internet based communications"*. 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 §§4.69-4.70) pointless; and the "in accordance with the law" test under Art. 8 cannot conceivably impose such a requirement.

4.71 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) Whilst a s. 8(4) warrant in principle permits interception of what is (at the point of interception) a substantial volume of communications to be intercepted, it is necessary that the communications actually sought are "external communications" of a particular description, which must be set out in the warrant: see s. 8(4). Further, interception will be targeted at communications "links" (to use Lord Bassam's wording). However, the legislative framework expressly authorises the interception of internal communications not identified in the warrant, to the extent that this is necessary to obtain the "external communications" that are the subject of the warrant: see s. 5(6)(a) RIPA; and (as Lord Bassam explained to Parliament, and given §1.36 above) is in practice inevitable that, when intercepting material at the level of communications links, both "*internal*" and "*external*" communications will be intercepted.

(2) Thus, the distinction between external and internal communications offers an important safeguard at a "macro" level, when it is determined what communications links should be targeted for interception under the s. 8(4) Regime. When deciding whether to sign a warrant under section 8(4) RIPA, the Secretary of State will – indeed must – select communications links for interception on the basis that they are likely to contain external communications of intelligence value, which it is proportionate to intercept. Moreover, interception operations under the s. 8(4) Regime are conducted in such a way that the interception of communications that are not external is kept to the minimum necessary to achieve the objective of intercepting wanted external communications (Mr 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.

4.72 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.

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

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

4.75 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 <u>not</u> 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 <u>express</u> modification to the certificate accompanying the section 8(4) warrant.

4.76 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[141].

<u>The breadth of the concepts of "national security" and "serious crime"</u>

[141] See 5 December Judgment, §101.

4.77 The Applicants complain about what they contend is the excessive breadth of the categories of "national security" and "serious crime" which they say "provides no meaningful restriction on the scope of the intelligence services' discretion to inspect intercepted material": see Additional Submissions at §46(2).

4.78 **First,** the Court 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 otherwise controlled by appropriate and sufficient safeguards. Most notably for present purposes, the applicant in *Kennedy* 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, just as the Applicants now contend; and that argument was rejected in terms by the Court at §159:

> "*As to the nature of the offences, the Court emphasises that the condition of foreseeability does not require states to set out exhaustively by name the specific offences which may give rise to interception. However, sufficient detail should be provided of the nature of the offences in question. In the case of RIPA, s.5 provides that interception can only take place where the Secretary of State believes that it is necessary in the interests of national security, for the purposes of preventing or detecting serious crime, or for the purposes of safeguarding the economic well-being of the United Kingdom. The applicant criticises the terms "national security" and "serious crime" as being insufficiently clear. The Court disagrees. It observes that the term "national security" is frequently employed in both national and international legislation and constitutes one of the legitimate aims to which art. 8(2) itself refers. The Court has previously emphasised that the requirement of "foreseeability" of the law does not go so far as to compel states to enact legislative provisions listing in detail all conduct that may prompt a decision to deport an individual on "national security" grounds. By the very nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance. Similar considerations apply to the use of the term in the context of secret surveillance. Further, additional clarification of how the term is to be applied in practice in the United Kingdom has been provided by the Commissioner, who has indicated that it allows surveillance of activities which threaten the safety or well-being of the state*

and activities which are intended to undermine or overthrow parliamentary democracy by political, industrial or violent means."

4.79 The reasoning of the Court in *Kennedy* is that the term "national security" has sufficient clarity without further definition, since threats to national security may be difficult to define in advance, and the term "national security" is one frequently applied in national and international legislation. That reasoning is unaffected by whether the Commissioner's statement is current. It also reflects a consistent line of Convention case law: see e.g. the admissibility decisions in *Esbester v United Kingdom app. 18601/91, Hewitt and Harman v United Kingdom app. 20317/92* and *Campbell Christie v United Kingdom app. 21482/93,* and the recent decision of the ECtHR in *RE v United Kingdom* app. 62498/11 (27 October 2015) at §133.

4.80 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[142]. In this case, for all the reasons already set out above at 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.

4.81 **Secondly,** the s.8(4) Regime is designed so as to ensure that a person's communications, intercepted under a s.8(4) warrant, cannot be examined simply 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:

[142] See too *Szabo and Vissy v Hungary app. 37138/14,* 12 January 2016, 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 unsufficiently 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."*)

(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 and §2.63 above.

(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 and §2.79 above.

(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 and §2.79 above.

4.82 **Finally**, in terms of the contention that the meaning of "serious crime" is insufficiently clear, 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 s. 81 RIPA.

4.83 In conclusion, for all the above reasons, the s.8(4) Regime is "in accordance with the law" for the purposes of Article 8 ECHR.

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

4.84 As to the question whether the s.8(4) Regime is "necessary in a democratic society" (see §§61-69 of the Applicants' Additional Submissions), the Court 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.

4.85 The Fourth Section has recently suggested in *Szabo and Vissy* (while acknowledging that this "represents at first glance a test different from the one prescribed in [Article 8(2)]") that measures of secret surveillance should be "strictly necessary" in two respects: (i) as a general consideration, for the safeguarding of democratic institutions; and (ii) as a particular consideration, for the obtaining of vital intelligence in an individual operation: see *Szabo,* §§72-73. It is submitted that the test previously set out by the Grand Chamber and in the other long-standing cases just referred to is to be preferred. It represents a properly protective set of principles which balance both 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. Strict necessity as a concept is used expressly in the Covention scheme – 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.

4.86 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.

4.87 **First,** the s.8(4) Regime contains adequate and effective guarantees against abuse for all the reasons already set out above for the purposes of the "in accordance with the law" test. If those guarantees render the regime "in accordance with the law" (as they do), they plainly satisfy the "necessity test" - not least, given the margin of appreciation available to the State in this area.

4.88 Thus, the safeguards ensure that material is not examined by reference to factors referable to an individual in the UK without the Secretary of State's approval; that the criteria for examining intercepted material are precise and focused, and access to it strictly controlled; that intercept does not occur on the basis of an over-broad

definition of national security; that the use of data both by the Intelligence Services and foreign agency counterparts is sufficiently controlled; and that there is proper judicial and other independent oversight.

4.89 **Secondly,** the s.8(4) Regime is indeed strictly necessary, as a general consideration, for the safeguarding of democratic institutions. The Applicants challenge the regime on the basis that GCHQ's "interception each day of millions of e-mails, Google messages and other data concerning internet use" is not proportionate (see eg. §67 of the Applicants' Additional Submissions). But that 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".

4.90 The first point here is that 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 communication links that are most likely to carry "external communications" meeting the descriptions of material certified by the Secretary of State, and will intercept only those links: 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 communication links, 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 communications link 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 link continues to be proportionate, but must also give an assessment of the intelligence value of material obtained

from the link to date (Code, §6.22).

4.91 If the Intelligence Services were unlawfully intercepting links 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 (***See Annex 11***).

4.92 Further, there are technical reasons why it is not possible to find a wanted communication travelling over a communications link without intercepting the entire contents of that link, and interrogating them automatically (if only for a very short period); and the pressing need to obtain external communications travelling over such links in the interests of national security is plain, on the basis of the findings in the ISC and Anderson Reports (see §§1.33-1.35 above).

4.93 Thus, the ISC has explained that bulk interception under the s.8(4) Regime is *"essential"* if the Intelligence Services are to discover threats effectively (see §2.25). That point is borne out by the examples given at Annex 9 to the Anderson Report (see §1.34 above), which record the discovery and/or successful disruption of major national security threats, in circumstances where bulk interception was the only means likely to have produced the desired intelligence. So if the Applicants wish to say that intercepting the contents of a communications link 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).

4.94 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 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 §§4.11-4.12 above.

4.95 **Thirdly,** the question of whether surveillance is necessary "*as a particular consideration, for the obtaining of vital intelligence in an individual operation*" (*Szabo* at §73) appears to relate to the facts of interception in a particular case, rather than to the applicable regime as a whole - thus, for example, to the question whether it corresponds to a pressing social need, and is proportionate, to issue a warrant covering a certain communications link. That question does not arise here, where the challenge is to the s.8(4) Regime *in abstracto*. However, at a systemic level, effective safeguards exist to ensure that (i) communications links are only accessed where necessary and proportionate for the purposes in the Secretary of State's certificate, which themselves must follow the intelligence priorities set by the NSC; and (ii) particular communications from those links can only be examined, if their examination is necessary and proportionate for those purposes. Indeed, in the context of bulk interception (which the Court has confirmed is lawful in principle in *Weber*), the test in *Szabo* can only relate to the stage at which communications are selected for examination: and at that stage, for all the reasons set out above, stringent controls are applied under s.8(4) Regime both as a matter of law and of fact to ensure that communications are only examined where it is necessary and proportionate to do so, because of the intelligence they contain.

Prior judicial authorisation of warrants

4.96 The Applicants contend that prior judicial authorisation of warrants is required for the s.8(4) Regime to be comply with Article 8 ECHR: see §68 of the Applicants' Additional Submissions. The Government strongly deny that the Convention requires or should require any such precondition. 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.

4.97 **First,** the Court'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:

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:

> *"The Court recalls that in Dumitru Popescu (cited above, §§70-73) it expressed the view that either the body issuing authorisations for interception should be independent or there should be control by a judge or an independent body over the issuing body's activity. Accordingly, in this field, control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception, warranting close scrutiny (see Klass and others, cited above, §§42 and 55). The ex ante authorisation of such a measure is not an absolute requirement per se, because where there is extensive post factum judicial oversight, this may counterbalance the shortcomings of the authorisation (see Kennedy, cited above, §167)."* (Emphasis added)

(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 Court's case law.)

4.98 **Secondly,** there is extensive independent (including judicial) *post factum* oversight of secret surveillance under the s.8(4) Regime. 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 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."

4.99 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 §§1.41-1.51 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 §2.111 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, [***See Annex 13***]).

Specific criticisms of IPT's Third Judgment (22 June 2015)

4.100 The applicants have made a number of specific criticisms of the IPT's third judgment dated 22 June 2015.

4.101 **First** it is said that the IPT failed to assess the general proportionality of the s. 8(4) regime and that there has been no proper consideration of that issue at the domestic level. But that is contrary to the express wording of the judgment of 22 June 2015 which made clear that the IPT considered proportionality both as it arose specifically in relation to the claimants' communications and as it arose in respect of the s.8(4) regime as a whole (what it referred to as "systemic proportionality") – see judgment at §3. In any event, for the reasons set out at §§4.84-4.95 above, the regime very clearly satisfies the "necessity" test. In that regard it is important that the s.8(4) regime is not one which can properly or accurately be characterised as one of "bulk

interception surveillance", contrary to the applicant's submissions on the third judgment at §§16-17 and for the reasons set out at §§1.19-1.28 above.

4.102 **Secondly** the applicants assert that the individual determinations in favour of two of the human rights organisations (Amnesty International and the Legal Resource Centre) in the Liberty proceedings are evidence that the UK intelligence services have "*deliberately targeted*" the communications of human rights organisations on the basis that they are "*national security targets*" (see §§18-25 of the applicants' submissions on the Third Judgment).

4.103 No such inference can possibly be drawn from the IPT's conclusions. The IPT found that GCHQ had lawfully and proportionately intercepted, and selected for examination, communications from or to particular email addresses associated with Amnesty International and the Legal Resources Centre; but (in the case of Amnesty International) breached its internal retention policy, and (in the case of the Legal Resource Centre) breached its internal policy on selection. The 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. Those conclusions do not imply, still less state, that GCHQ "*deliberately targeted the communications of human rights organisations*" or that "*the government deems that human rights NGOs may legitimately be considered "national security targets*[143]*""*. The IPT was self-evidently aware of the necessary tests which had to be satisfied in order to reach its conclusions, it having set out the requirements of the s.8(4) regime in detail in the 5 December 2014 judgment and having repeated its conclusions at §4 of the 22 June judgment (see in particular at §4(i)(a)). Those tests included the requirement that the selection of communications for examination be necessary and proportionate, and that those communications fall into a category set out in the Secretary of State's certificate under s.5 RIPA. Had the Intelligence Agencies been deliberately targeting human rights organisations in an unlawful/indiscriminate way the IPT would have so stated.

[143] See Submissions, §25.

4.104 **Thirdly** 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/selection 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 carry out its functions in such a way as 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 that important rule. As is clear from the Art. 6 case law discussed separately in these Observations (See §7.11-7.31), that there can be circumstances in which it is lawful for material to be withheld on eg. national security grounds, without prejudicing the fairness of the proceedings, is well established. Particularly in circumstances where the IPT had the assistance of CTT (acting in the role of special advocate) to represent the interests of the applicants in the closed proceedings, it cannot be said that this renders the proceedings in breach of Art. 6 (which is what appears to be being implied in this part of the applicants' submissions).

4.105 **Fourthly** the applicants assert that there was a failure to address Art. 10 ECHR in the third judgment. But the applicants do not indicate 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.

4.106 In addition there is no merit in the complaint 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. This is addressed at §§134-135 of the IPT's 5 December judgment. As is evident from that extract from the judgment:

(1) Liberty only sought to raise, at a very late stage of the IPT proceedings (in written submissions dated 17 November 2014), the issue whether there was adequate provision under Art. 10 ECHR for dealing with confidential information in the context of NGO activities ('NGO confidence');
(2) The issue of NGO confidence was not raised when the legal issues were agreed between all parties on 14 February 2014, some 5 months before the open legal issues hearing in July 2014;
(3) The written arguments addressed at the July 2014 hearing had not raised any separate issue under Art. 10 ECHR in respect of NGO confidence.
(4) Liberty had been given ample opportunity to raise the issue, but had not done so.
(5) The IPT concluded that it was far too late (in November 2014) to be seeking to raise the issue, particularly in circumstances where it was being suggested that further disclosure and "considerable" further argument would be necessary to incorporate it into the proceedings at that stage.

4.107 **Fifthly**, the applicants criticise the IPT for failing to make clear whether the "accessing" of Amnesty's communications involved its communications data and/or whether the communications data of the Legal Resource centre was analysed following its selection for examination. But this criticism is 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 would have said so in its judgment.

4.108 **Finally** the applicants have submitted that the IPT's correction to its judgment, in which it substituted Amnesty for the Egyptian Initiative for Personal Rights "undermines the Tribunal's earlier findings that the UK surveillance regime contains adequate safeguards to protect fundamental rights". These submissions are not understood. The IPT made clear in its letter dated 1 July 2015 that there had been a mistaken attribution in the judgment which did not result from any failure by the Respondents to make disclosure. That is not a matter which can appropriately lead to the criticism that it demonstrates a lack of rigour in the Tribunal's proportionality assessment. The IPT's judgment (including its proportionality assessment) was

reached after full consideration of the relevant material in closed sessions, where the applicants' interests were represented by CTT, acting in effect as a special advocate.

5 QUESTION 3. ARTICLE 8 - IMPACT OF THE FACT THAT APPLICANTS ARE NON-GOVERNMENTAL ORGANISATIONS ('NGOS')

5.1 It is submitted that the applicants' status as NGOs makes no material difference to the principles to be applied in determining whether the Intelligence Sharing or the s.8(4) Regime violates their rights under Art. 8 (or Art. 10) of the Convention.

5.2 The Applicants' principal challenge is to the lawfulness of the Intelligence Sharing and s.8(4) Regimes in general and, save for the issue of prior judicial authorisation which is raised in the context of Art. 10 ECHR and the s.8(4) Regime (see below), the Applicant's have not suggested that their status as Non-Governmental Organisations (NGOs) makes a material difference to the tests to be applied when considering the lawfulness of the Regimes (see the Applicants' Additional Submissions on the Facts and Complaints at §§41-73).

5.3 The Government accepts that it is possible for material emanating from NGOs to be intercepted in the course of the execution of a s.8(4) warrant. It is also possible that some of that material may be of a sensitive or privileged nature. The same applies to other categories of confidential information which may be included within 'external communications' intercepted under the s.8(4) Regime. However, in the context of a regime of strategic monitoring such as the s.8(4) Regime, which does not target NGO (or journalistic) material (whether for the purposes of identifying sources or otherwise) there is no material distinction to be drawn between NGO material and other types of material which may also be subject to untargeted interception.

5.4 In any event there are special provisions in the Code addressing the handling of confidential material as set out in detail below in the context of Art. 10 ECHR (see §§ 6.24-6.28 below)

6 *QUESTION 4. ARTICLE 10 - THE CONVENTION PROTECTION AFFORDED TO NGOS UNDER ART. 10 ECHR*

6.1 In the light of the cases cited at §38 of *Guseva v Bulgaria*, Appl. No. 6987/07, 17 February 2015, including *Österreichische Vereinigung zur Erhaltung v. Austria*, Appl. No. 39534/07, 28 November 2013 (see in particular §§33-34), the NGOs engaged in the legitimate gathering of information of public interest in order to contribute to public debate may properly claim the same Art. 10 protections as the press. In principle, therefore, the obtaining, retention, use or disclosure of the applicants' communications and communications data may potentially amount to an interference with their Art. 10 rights, at least where the communications in question are quasi-journalistic ones, relating to their role as "social watchdogs".

The requirements of Art. 10

6.2 Although the Court has formulated a separate question addressing the merits of the applicants' case under Art. 10 of the Convention, the applicable principles are materially the same as those addressed above under Art. 8.

6.3 The only respect in which the applicants seek to contend that Art. 10 may give rise to an additional argument over and above the tests under Art. 8 is in respect of prior judicial authorisation for s. 8(4) warrants under the s.8(4) Regime (see §68 and §§78-81 of the Additional Submissions on the Facts and Complaints). That is consistent with the applicants' position during the domestic IPT proceedings where (save for the question of prior judicial authorisation under Art. 10) it was agreed between the parties that no separate argument arose in relation to Article 10(2), over and above that arising out of Article 8(2) (see the IPT's 5 December judgment at §149).

6.4 The cases to which the Court has referred in its question – *Nordisk Film*[144], *Financial Times Ltd*[145], *Telegraaf Media* and *Nagla* – are all cases concerned with targeted measures directed to the identification and/or disclosure of journalistic sources. None of them is concerned with strategic monitoring of the type conducted under the s.8(4) Regime. These cases are, therefore, to be distinguished from *Weber*,[146] and

[144] *Nordisk Film & TV A/S v Denmark* App. No. 40485/02, 8 December 2005.
[145] *Financial Times Ltd and Others v the United Kingdom*, App. No. 821/03, 15 December 2009; (2010) 50 EHRR 1153.
[146] *Weber and Saravia v Germany* (2008) 46 EHRR SE 47

the principles it identified as being applicable to a strategic monitoring regime which did not target journalistic material.

6.5 In light of the question asked by the Court, and the extent to which the applicants appear to place particular reliance on their status as NGOs (as entitling them to the same protection as journalists under Art. 10), the submissions set out below address the following three issues:

(i) Whether there is any material difference, in a case of this nature, between the principles to be applied under Article 8 and Article 10 when determining whether the measures in question are in accordance with the law/prescribed by law.

(ii) Whether the possibility that confidential journalistic (or NGO) material might be intercepted in the course of strategic monitoring under the s.8(4) Regime gives rise to considerations under Article 10 which have not been fully addressed in the analysis of Article 8 above.

(iii) Whether the particular nature of confidential journalistic (or NGO) material gives rise to a requirement for prior judicial oversight in the context of the s.8(4) regime.

The Applicable Principles

6.6 Although there is a difference in the English text of the Convention between the wording of the material provisions of Article 8 ('in accordance with the law') and Article 10 ('prescribed by law'), the Court has observed, in *Telegraaf Media*, that there is no difference in the French text which includes the formulation '*prevue(s) par la loi*' in both Articles (§89).

6.7 In §90 of *Telegraaf Media* the Court made clear that the essential requirements of Article 8(1) and Article 10(1) were the same:

> "*The Court reiterates its case-law according to which the expression "in accordance with the law" not only requires the impugned measure to have some basis in domestic law, but also refers to the quality of the law in question, requiring that it should be accessible to the person concerned and foreseeable as to its effects. The law must be*

compatible with the rule of law, which means that it must provide a measure of legal protection against arbitrary interference by public authorities with the rights safeguarded by Article 8 § 1 and Article 10 § 1."

6.8 The Government therefore adopts, but does not repeat, the observations set out above as to why the s.8(4) Regime is 'in accordance with the law' for the purposes of Article 8(2).

6.9 The test of 'necessity' in a democratic society is common to both Article 8(2) and Article 10(2). The applicants do not contend that a different approach should be taken to the assessment of necessity under the two Articles. The Government therefore adopts, but does not repeat, the observations set out above as to why the s.8(4) Regime is 'necessary in a democratic society' for the purposes of Article 8(2).

Interception of Journalistic Material

6.10 The Court has drawn a sharp, and important, distinction between measures that target journalistic material, particularly for the purpose of identifying sources, and strategic monitoring of communications (and/or communications data). Thus, at §151 of *Weber*:

"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 characterised as particularly serious."

6.11 Accordingly, Article 10 adds nothing of substance to the Article 8 analysis in a case concerned with strategic monitoring. The interference with freedom of expression consequent upon such monitoring is not '*particularly serious*' and any such limited interference will be justified under Article 10(2) for the same reasons that it is justified under Article 8(2). Put differently, Article 10(2) will not require, in the case

of untargeted strategic monitoring, an enhanced level of justification in respect of confidential journalistic material beyond that which Article 8(2) will require in respect of private and/or confidential communications (and/or communications data) of different types.

6.12 The line of cases identified by the Court in its question concern a different issue, namely the application of targeted measures to individual journalists for the purposes of source identification. For obvious reasons, the Court has adopted a different approach to cases of this nature. It has repeatedly emphasised the 'potentially chilling effect' that measures which compel the identification of journalistic sources may have on the ability of the press effectively to fulfil its important 'public-watchdog' role. In light of those concerns it has set a more demanding threshold of justification for such measures.

6.13 The importance of the distinction between the 'not particularly serious' interference caused by strategic monitoring and the 'potentially chilling effect' of measures directed to source disclosure is clearly illustrated by the Court's reasoning in *Telegraaf Media.* Having determined that the 'special powers' exercised in respect of the applicants were accessible, foreseeable, and subject to sufficient safeguards, so as to be 'in accordance with the law', the Court addressed (at §95 et seq.) the applicants' contention that their status as journalists required special safeguards to ensure adequate protection of their journalistic sources.

6.14 The Court commenced its analysis of this issue by considering whether its reasoning in *Weber* was applicable. The critical feature of the measures considered in *Weber* was identified as being that they were properly to be characterised as 'strategic monitoring', for the principal purpose of identifying and averting dangers in advance. They were not targeted at journalists and they did not have the identification of journalistic sources as their aim. That being so, the interference with freedom of expression consequent upon the measures in question was not to be regarded as particularly serious, and there was no requirement for special provision for the protection of press freedom.

6.15 The Court then observed that the situation in *Telegraaf Media* was materially different to that considered in *Weber*. The difference was expressed as follows (at §97):

> *"The present case is characterised precisely by the targeted surveillance of journalists in order to determine from whence they have obtained their information. It is therefore not possible to apply the same reasoning as in Weber and Saravia."*

6.16 The distinction between strategic monitoring of the type addressed in *Weber*, and targeted measures specifically directed at the identification of journalistic sources, and the reasons for that distinction, are further explained in the Court's analysis of the second aspect of the applicants' complaint in *Telegraaf Media* namely the order to surrender documents. The potentially 'chilling effect' of such an order on press freedom was described by the Court in the following terms, at §127:

> *"Protection of journalistic sources is one of the basic conditions for press freedom, as is recognised and reflected in various international instruments including the Committee of Ministers Recommendation quoted in paragraph 61 above. Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public-watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected. Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society and the potentially chilling effect an order of source disclosure has on the exercise of that freedom, such a measure cannot be compatible with Article 10 of the Convention unless it is justified by an overriding requirement in the public interest (see* Goodwin*, cited above, § 39;* Voskuil*, cited above, § 65;* Financial Times Ltd. and Others*, cited above, § 59; and* Sanoma*, cited above, § 51)."*

6.17 The potentially 'chilling effect' identified in *Telegraaf Media* derived from the act of 'source disclosure'. Similarly, in *Goodwin*[147], a case concerned with a court order requiring a journalist to surrender documents for the specific purpose of identifying one of his sources, the Court identified the potentially 'chilling effect' of such a measure as arising specifically from the order for disclosure (at §39), in contrast to

[147] *Goodwin v United Kingdom* (1996) 22 EHRR 123

some general possibility that a journalistically privileged communication might fall into the hands into the authorities in the course of a programme of strategic monitoring:

> *"Protection of journalistic sources is one of the basic conditions for press freedom, as is reflected in the laws and the professional codes of conduct in a number of Contracting States and is affirmed in several international instruments on journalistic freedoms (see, amongst others, the Resolution on Journalistic Freedoms and Human Rights, adopted at the 4th European Ministerial Conference on Mass Media Policy (Prague, 7-8 December 1994) and Resolution on the Confidentiality of Journalists' Sources by the European Parliament, 18 January 1994, Official Journal of the European Communities No. C 44/34). Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public-watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected. Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society and the potentially chilling effect an order of source disclosure has on the exercise of that freedom, such a measure cannot be compatible with Article 10 (art. 10) of the Convention unless it is justified by an overriding requirement in the public interest."*[148]

6.18 In *Financial Times*, the Court, observed (at §70) that although the disclosure order in that case concerned material which 'might, upon examination' lead to source identification, and would not necessarily lead to such identification, the distinction was not a material one. The 'chilling effect' would arise '*wherever journalists are seen to assist in the identification of anonymous sources*.'

6.19 The Court returned to this issue in *Nagla*. That case concerned a search by police of a journalist's house and seizure of her date storage devices following a broadcast she had aired informing the public of an information leak from the State Revenue database. The applicant complained that she had been compelled to disclose information that had enabled a journalistic source to be identified, in violation of her right to receive and impart information as protected by Article 10. The Court held

[148] See, also *Voskuil v Netherlands* [2004] EMLR 14 465 at §65.

that the complaint fell within the sphere of protection provided by Article 10 and expressed its concern as to the potential chilling effect on press freedom in the following terms, at §82:

> *"The Court notes that the Government admitted that the search at the applicant's home had been aimed at gathering "information about the criminal offence under investigation" and that it authorised not only the seizure of the files themselves but also the seizure of "information concerning the acquisition of these files". While recognising the importance of securing evidence in criminal proceedings, the Court emphasises that a chilling effect will arise wherever journalists are seen to assist in the identification of anonymous sources (see Financial Times Ltd and Others v. the United Kingdom, no. 821/03, § 70, 15 December 2009)."*

6.20 The case of *Nordisk*, referred to by the Court in its questions, adds nothing material to this analysis. On the particular facts of *Nordisk* the material in question was regarded as consisting of the applicant's 'research material' rather than material provided by journalistic sources. The Court considered that Article 10 might be applicable in a case involving such material, observing that '*a compulsory hand over of research material may have a chilling effect on the exercise of journalistic freedom of expression*.' As with the 'journalistic source' cases addressed above, the 'chilling effect' derives from the 'handing over' of the material by the journalist to the authorities.

6.21 The Court has been clear and consistent in its identification of the potentially 'chilling effect' that may arise from the disclosure of journalistically privileged material. The potential danger arises in circumstances where the journalist is seen to assist (whether under compulsion or otherwise) in the identification of anonymous sources, and thereby infringe the duty of confidence owed by a journalist to his or her source. That is not a situation that arises in the course of the operation of the s.8(4) Regime. To the extent that journalistically privileged or NGO material may be intercepted under the s.8(4) Regime, that interception takes place without any active involvement (or 'assistance') on the part of the journalist/NGO concerned. The s.8(4) Regime does not concern 'source disclosure' of the type addressed in *Telegraaf Media*, *Nagla* and the line of earlier cases of a similar nature summarised above.

6.22 It is the potentially chilling effect on press freedom, and the ability of the press to perform its 'vital public-watchdog' role, that founds the proposition that any order for disclosure, or other measure targeted at the identification of a journalistic source, must be justified by 'an overriding requirement in the public interest.' The consistent approach of the Court in this context falls to be contrasted with the approach it has taken to non-targeted, strategic monitoring in respect of which the interference with journalistic freedom of expression is not to be regarded as 'particularly serious.'

6.23 As observed by the Court in *Weber* (at §151), in the context of a regime of strategic monitoring, which is not targeted to the communications of journalists (or any other group) it will only be when an intercepted communication is selected for examination that it will (or may) become apparent that the communication contains journalistic material. The Code contains a number of specific safeguards directed to preserving the confidentiality of journalistic material in such circumstances.

6.24 In fact, and notwithstanding the submissions set out above, the s.8(4) Regime does include special provisions in respect of journalistic and confidential information. At §4.2 of the Code it states:

> "*Particular consideration should also be given in cases where the subject of the interception might reasonably assume a high degree of privacy, or where confidential information is involved. This includes where the communications relate to legally privileged material; where confidential journalistic material may be involved; where interception might involve communications between a medical professional or Minister of Religion and an individual relating to the latter's health or spiritual welfare; or where communications between a Member of Parliament and another person on constituency business may be involved.*"[149]

As is evident from the first sentence above, the requirement for "particular consideration" applies to any material where the subject of the interception might assume a high degree of privacy or where confidential information is involved and the Code does not provide an exhaustive definition of when material will fall into that category.

[149] And similar provisions were to be found in the 2002 Code see §§3.2-3.11.

6.25 In addition the definition of "confidential journalistic material" is a broad one under the Code. At §4.3 it states:

> "*Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking...*"

6.26 At §4.32, the Code states that the safeguards set out in § 4.28-4.31 are to be applied to any s.8(4) material which is selected for examination and which constitutes confidential information (including confidential journalistic material). The material elements of Code requiring as follows:

> *"4.29. Material which has been identified as confidential information should be retained only where it is necessary and proportionate to do so for one or more of the authorised purposes set out in section 15(4). It must be securely destroyed when its retention is no longer needed for those purposes. If such information is retained, there must be adequate information management systems in place to ensure that continued retention remains necessary and proportionate for the authorised statutory purposes.*
> *4.30. Where confidential information is retained or disseminated to an outside body, reasonable steps should be taken to mark the information as confidential. Where there is any doubt as to the lawfulness of the proposed handling or dissemination of confidential information, advice should be sought from a legal adviser within the relevant intercepting agency and before any further dissemination of the material takes place.*
> *4.31. Any case where confidential information is retained should be notified to the Interception of Communications Commissioner as soon as reasonably practicable, as agreed with the Commissioner. Any material which has been retained should be made available to the Commissioner on request."*

6.27 Although the applicants do not appear to raise any separate, specific complaint as regards the Intelligence Sharing Regime and NGO confidence, it is to be noted that in Chapter 12 of the Code it makes clear that such material is to be handled in the same

way as material which is obtained directly by the Intelligence Agencies (see §12.6[150]) i.e. the same safeguards as set out above would apply to confidential material including confidential journalistic material obtained pursuant to the Intelligence Sharing Regime (see **§**6.26).

6.28 Accordingly there are detailed provisions of the Code which provide special protection for confidential material including confidential journalistic material.

6.29 To this extent, the safeguards under the s.8(4) Regime are more rigorous than those considered to be sufficient by the Court in *Weber.* At §151, the Court noted that there were no 'special rules' forming part of the regime under the G10 Act as to how journalistic material should be treated in the event that such material was selected for examination. However, it did not regard such rules as necessary in light of the general safeguards forming part of the scheme as a whole:

> *"It is true that the impugned provisions of the amended G10 Act did not contain special rules safeguarding the protection of freedom of the press and, in particular, the non-disclosure of sources, once the authorities had become aware that they had intercepted a journalist's conversation. However, the Court, having regard to its findings under Art.8 , observes that the impugned provisions contained numerous safeguards to keep the interference with the secrecy of telecommunications – and therefore with the freedom of the press – within the limits of what was necessary to achieve the legitimate aims pursued. In particular, the safeguards which ensured that data obtained were used only to prevent certain serious criminal offences must also be considered adequate and effective for keeping the disclosure of journalistic sources to an unavoidable minimum. In these circumstances the Court concludes that the respondent State adduced relevant and sufficient reasons to justify interference with freedom of expression as a result of the impugned provisions by reference to the legitimate interests of national security and the prevention of crime. Having regard*

[150] Which provides, as follows: "*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… and communications data… 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.*"

to its margin of appreciation, the respondent State was entitled to consider these requirements to override the right to freedom of expression."

6.30 Whilst the specific safeguards set out in the Code in relation to confidential material may not be necessary to ensure compliance with Articles 8 and/or 10 in the context the s.8(4) Regime of strategic monitoring, the fact that such safeguards exist is clearly sufficient to address any assertion by the applicants that specific safeguards are required in respect of NGO material where the applicants are in communication with sources (see §78 of the applicants' Additional Submissions on the Facts and Complaints).

Prior Judicial Authorisation

6.31 As already noted, the Court's case law does not require independent authorisation of warrants as a precondition of the lawfulness of interception of communications (or communications data), provided that the applicable regime otherwise contains sufficient safeguards: see §§4.96-4.97 above.

6.32 Nor has the Court established a rule requiring prior judicial authorisation for state interference with journalistic freedom. In some cases prior judicial scrutiny has been found to be necessary, in others it has not.

6.33 In *Sanoma Uitgevers BV v The Netherlands*[151], the Court was concerned with a Dutch law authorising the compulsory surrender of material to the police for use in a criminal investigation. It was, therefore, a case concerned with targeted measures to compel disclosure of journalistic sources (such as *Goodwin, Financial Times*, and *Telegraaf Media*) rather than a regime of strategic monitoring in the course of which journalistic material might be intercepted (*Weber*). It was in this context that the Court identified the importance of prior authorisation by a Judge or other independent body:

"89. The court notes that orders to disclose sources potentially have a detrimental impact, not only on the source, whose identity may be revealed, but also on the

[151] [2011] EMLR 4

newspaper or other publication against which the order is directed, whose reputation may be negatively affected in the eyes of future potential sources by the disclosure, and on members of the public, who have an interest in receiving information imparted through anonymous sources …

92. Given the preventive nature of such review the judge or other independent and impartial body must thus be in a position to carry out this weighing of the potential risks and respective interests prior to any disclosure and with reference to the material that it is sought to have disclosed so that the arguments of the authorities seeking the disclosure can be properly assessed."

6.34 Similarly, in *Telegraaf Media*, another case concerned with the targeted measures directed against journalists with a view to obtaining knowledge of their sources, the Court considered that a post factum review was insufficient in circumstances where, once the confidentiality of journalistic sources had been destroyed, it could not be repaired. The Court's conclusion was expressly tied to the nature and purpose of the powers being exercised, (at §102):

"The court thus finds that the law did not provide safeguards appropriate to the use of powers of surveillance against journalists with a view to discovering their journalistic sources. There has therefore been a violation of articles 8 and 10 of the Convention.

6.35 The Court of Appeal in *Miranda*[152] considered the judgment of the Court in *Nagla*, and decided that it supported the proposition that a requirement for prior judicial authorisation could extend beyond cases involving source disclosure to cases concerned with the seizure of a journalist's material, such as computers, hard drives and memory cards. It was observed (at §113) that such seizure of journalistic material, even if not directly concerned with the identification of a source, could serve to create a 'chilling effect' of a similar nature to that created by measures expressly directed to source identification.

6.36 The extent to which an order permitting the seizure of journalistic material, for purposes other than source identification, will have a chilling effect on the freedom

[152] *R (Miranda) v Secretary of State for the Home Department* [2016] EWCA Civ 6 (See Annex 54).

of journalistic expression is likely to depend on the facts of the case and the Court has adopted a carefully fact-sensitive approach to cases of this nature. However, there is clearly a material difference between an order specifically directed to the seizure of (for example) a journalist's computer and the operation of a strategic monitoring regime under which a journalist's communications (or communications data) may be intercepted in the course of a large-scale and untargeted programme of interception.

6.37 There is no authority in the Court's caselaw[153] 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. The only circumstances in which such a requirement has been found to exist is in respect of targeted measures directed at the identification of journalistic sources and/or the seizure of journalist's material.

6.38 Even if it were considered desirable in principle, a requirement of prior judicial authorisation in the operation of the s.8(4) Regime would be of no practical effect, as observed by the IPT in the Liberty proceedings in the 5 December judgment, 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."*

[153] Or the domestic case law for that matter.

6.39 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.

7 QUESTION 5: ARTICLE 6 OF THE CONVENTION

The rights at issue are not "civil rights".

7.1 In *Klass*, the Commission (Report of the Commission, Series B, no. 26 pp35-37) 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). In particular, it held at §58:

> *"...to determine what is the scope meant by 'civil rights' in Art. 6, some account must be take 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."*

7.2 The Court approved this conclusion in *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. Consequently it is clear that Art. 6 did not apply to the domestic IPT proceedings[154].

[154] It is to the noted that the IPT's own conclusion to the contrary in its Preliminary Issues Ruling in *Kennedy* (IPT/01/62) dated 9 December 2004, at §§85-108 was issued before the Court's judgment in *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* .

7.3 That conclusion is also consistent with the Court's reasoning in *Klass* in relation to the issue of judicial control of interception powers – see §§57-58[155]. Since the Convention must be read as a whole, the applicants' Art. 6 complaints in *Klass* had to be addressed in a manner that was consistent with the Court's conclusion on the appropriateness of judicial control under Art. 8. Accordingly, as regards Article 6 the Court held at §75:

> *"The Court has held that in the circumstances of the present case the G 10 does not contravene Article 8 in authorising a secret surveillance of mail, post and telecommunications subject to the conditions specified...*
>
> *Since the Court has arrived at this conclusion, the question whether the decisions authorising such surveillance under the G 10 are covered by the judicial guarantee set forth in Article 6 – assuming this Article to be applicable – must be examined by drawing a distinction between two stages: that before, and that after, notification of the termination of surveillance.*
>
> *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,*

[155] Where the Court stated:

> *"... it is necessary to determine whether judicial control, in particular with the individual's participation, should continue to be excluded even after surveillance has ceased. Inextricably linked to this issue is the question of subsequent notification, since there is in principle little scope for recourse to the courts by the individual concerned unless he is advised of the measures taken without his knowledge and thus able retrospectively to challenge their legality. 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'. Moreover, it is to be recalled that, in pursuance of the Federal Constitutional Court's judgment of 15 December 1970, the person concerned must be informed after the termination of the surveillance measures as soon as notification can be made without jeopardising the purpose of the restriction..."*

within the meaning of Article 6; as a consequence, it of necessity escapes the requirements of that Article.

The decision can come within the ambit of the said provision only after discontinuance of the surveillance. According to the information supplied by the Government, the individual concerned, once he has been notified of such discontinuance, has at his disposal several legal remedies against the possible infringements of his rights; these remedies would satisfy the requirements of Article 6 ...

The Court accordingly concludes that, even if it is applicable, Article 6 has not been violated."

7.4 The Court's judgment in *Klass* thus establishes that the requirements of Art. 6 cannot apply to a dispute concerning the interception powers insofar as the use of such powers in the case at issue remains validly secret (see the highlighted words in the passage above)[156].

7.5 The applicants' case clearly falls within the scope of this finding. During the domestic IPT proceedings the applicants' case was that there was a continuing situation of intelligence sharing/interception; it was not contended that there had been such interferences in the past and that the applicants could now be safely notified of that fact. Consequently at the time of the IPT proceedings, the Government adopted a stance of "neither confirm nor deny" (see §4(ii) of the 5 December judgment) and the legal issues were determined on the basis of hypothetical facts. Applying *Klass*, this was not a situation where Art. 6 applied.

7.6 The Court's conclusion in *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* that the rights at issue in the field of secret interception powers are not "civil" rights is further supported by the Court's more general jurisprudence on the meaning of "civil rights and obligations".

[156] 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).

7.7 As the Grand Chamber confirmed at §28 of *Ferrazzini v Italy* app. 44759/98, 12 July 2001, the mere fact that an individual enjoys rights or owes obligations does not in itself mean that those rights and obligations are "civil" for the purposes of Art. 6. The text of Art. 6 cannot be interpreted as if the adjective "civil" were not present (*Ferrazzini* at §30). It is clear that secret powers of intelligence gathering/interception that are used solely in the interests of national security or to detect serious crime, form part of the "*hard core of public-authority prerogatives*" so as to render it inappropriate to classify any related rights and obligations as "civil" in nature – see *Ferrazzini* at §§27-29[157] (and see also the reference to "discretionary powers intrinsic to state sovereignty" at §61 of *Vilho Eskelinen v Finland*, app. 63235/00, 19 April 2007).

7.8 Further, merely showing (or simply asserting) that a dispute is "pecuniary" in nature is not, in itself, sufficient to attract the applicability of Art. 6(1) under its "civil" head, see §25 of *Ferrazzini*. It follows, *a fortiori*, that the mere fact that in the IPT proceedings the Applicants' claimed, among other remedies, financial compensation, does not mean that Art. 6 is applicable to those IPT proceedings. Similarly, as the

---

[157] Where the Court stated, *inter alia*:

> "*27. Relations between the individual and the State have clearly evolved in many spheres during the fifty years which have elapsed since the Convention was adopted, with State regulation increasingly intervening in private-law relations. This has led the Court to find that procedures classified under national law as being part of "public law" could come within the purview of Article 6 under its "civil" head if the outcome was decisive for private rights and obligations, in regard to such matters as, to give some examples, the sale of land, the running of a private clinic, property interests, the granting of administrative authorisations relating to the conditions of professional practice or of a licence to serve alcoholic beverages...*
>
> *28. However, rights and obligations existing for an individual are not necessarily civil in nature. Thus, political rights and obligations, such as the right to stand for election to the National Assembly (see Pierre-Bloch, cited above, p. 223, § 50), even though in those proceedings the applicant's pecuniary interests were at stake (ibid., § 51), are not civil in nature, with the consequence that Article 6 § 1 does not apply…. Similarly, the expulsion of aliens does not give rise to disputes (contestations) over civil rights for the purposes of Article 6 § 1 of the Convention, which accordingly does not apply (see Maaouia, cited above, §§ 37-38).*
>
> *29. In the tax field, developments which might have occurred in democratic societies do not, however, affect the fundamental nature of the obligation on individuals or companies to pay tax. In comparison with the position when the Convention was adopted, those developments have not entailed a further intervention by the State into the "civil" sphere of the individual's life. The Court considers that tax matters still 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…*"

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

7.9 Finally, the fact that the Applicants had the right, as a matter of domestic law, to complain to the IPT does not 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) and thus it cannot be interpreted solely by reference to the domestic law of the respondent State. In addition the Tribunal is specifically designed to operate under the constraints recognised by the Court at §57 of *Klass* (and upon which the Court's conclusion in *Klass* under Art. 6 was based). In particular, 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: eg. the fact of any interception remains secret throughout (save, of course, where the Tribunal finds unlawfulness to have occurred). Thus the fact that RIPA offers individuals the additional safeguard (under Art. 8) of an unlimited right to complain to the Tribunal cannot in itself make Art. 6 apply to such disputes.

If the proceedings did involve the determination of "civil, rights", were the restrictions in the IPT proceedings, taken as a whole, disproportionate or did they impair the very essence of the applicants' right to a fair trial? (see Kennedy v the United Kingdom, no 26839/05, §186, 18 May 2010)

7.10 In the alternative, even if Art. 6 did apply to the proceedings before the IPT, it was satisfied. The IPT's procedures, which must take account of the legitimate need, based in national security, for the protection so sensitive information, plainly did not impair the very essence of the applicants' right to a fair trial, particularly given the Court's conclusions in the *Kennedy* case.

(1) Article 6 - the core principles

Disclosure rights not absolute

7.11 It is well established that although the right to a fair process is unqualified, the constituent elements or requirements of a fair process are not absolute or fixed: see *Brown v Stott* [2003] 1 AC 681 at 693D-E per Lord Bingham (See Annex 60); 719G-H per Lord Hope; 727H per Lord Clyde. In *Brown v Stott*, Lord Bingham stated at 704D:

> "*The jurisprudence of the European court very clearly establishes that while the overall fairness of a criminal trial cannot be compromised, the constituent rights comprised, whether expressly or implicitly, within article 6 are not themselves absolute*."

7.12 The approach of the Court in considering issues of fairness is therefore context and fact sensitive. This was re-affirmed by the Court in *A & Others v United Kingdom*, no. 3455/05, §203, 19 February 2009, when considering the requirements of Article 5(4). The Court stated in terms:

> "*The requirement of procedural fairness under Article 5(4) does not impose a uniform unvarying standard to be applied irrespective of the context, facts and circumstances*."

a. The context specific nature of the analysis of the requisite ingredients of fairness was emphasised at §217. The Court specifically tied its conclusions as to the ingredients of fairness to the particular context of that case:

> "*in the circumstances of the present case, and in view of the dramatic impact of the lengthy – and what appeared at that time to be indefinite – deprivation of liberty on the applicants' fundamental rights, Article 5(4) must import substantially the same fair trial guarantees as Article 6(1) in its criminal aspect*."
>
> Further at §220 the Court reinforced that each case must be considered on a "case-by-case basis", in line with its conclusion at §203.

7.13 This approach of the Court has been acknowledged by the domestic courts. In *R v H* [2004] 2 AC 134 (See Annex 61), Lord Bingham noted at §33:

"*The consistent practice of the Court, in this and other fields, has been to declare principles, and apply those principles on a case-by-case basis according to the particular facts of the case before it, but to avoid laying down rigid or inflexible rules. … It is entirely contrary to the trend of Strasbourg decision-making to hold that in a certain class of case or when a certain kind of decision has to be made a prescribed procedure must always be followed*."

7.14 The approach of the Court also acknowledges that the necessary ingredients of fairness can, and should, take into account what is at stake both for the individual concerned and for the general community. Consistently with this approach, the Court has recognised that the ingredients of fairness in the civil context may be different to i.e. lighter than and more flexible than those that apply in the criminal context: *Dombo Beheer v The Netherlands*, no. 14448/88, §32, 27 October 1993. That is also recognised in the structure and content of Article 6 itself: see Articles 6(2) and (3) ECHR. As stated in *Vanjak v Croatia*[158] at §45:

"*The requirements inherent in the concept of fair hearing are not necessarily the same in cases concerning the determination of civil rights and obligations as they are in cases concerning the determination of a criminal charge. This is borne out by the absence of detailed provisions such as paragraphs 2 and 3 of Article 6 applying to cases of the former category. Thus, although these provisions have a certain relevance outside the strict confines of criminal law (see, mutatis mutandis, Albert and Le Compte v. Belgium, 10 February 1983, Series A no. 58, § 39), the Contracting States have greater latitude when dealing with civil cases concerning civil rights and obligations than they have when dealing with criminal cases (see Pitkänen v. Finland, no. 30508/96, § 59, 9 March 2004).*"

7.15 Accordingly, very considerable caution is needed before concluding that an ingredient considered necessary in a context at one end of the spectrum (eg. a criminal case or a case involving deprivation or severe restriction of liberty) is also necessary in a context at the other end of the spectrum (eg. a complaint of unlawful interception in breach of qualified rights under the Convention).

[158] Application no. 29889/04 dated 14 January 2010

7.16 As to **disclosure**, in *Rowe and Davis v United Kingdom*, no. 28901/95, 16 February 2000 a criminal case, the Court stated at [60]:

> "*It is a fundamental aspect of the right to a fair trial that criminal proceedings, including the elements of such proceedings which relate to procedure, should be adversarial and that there should be equality of arms between the prosecution and defence. The right to an adversarial trial means, in a criminal case, that both prosecution and defence must be given the opportunity to have knowledge of and comment on the observations filed and the evidence adduced by the other party. In addition, Article 6(1) requires, as indeed does English law, that the prosecution authorities should disclose to the defence all material evidence in their possession for or against the accused*."

7.17 Whilst the general right to disclosure of the case against the individual and of the relevant evidence is clearly established "in a criminal case", even in that context the general right is not absolute. It is not one of the express procedural rights set out in Art. 6. The general right is implied into Article 6 as an aspect of the express right to a fair trial. Implied rights are in principle subject to necessary and proportionate restrictions.

7.18 It follows that the Court has held that the right to disclosure can be limited by reference to the rights and interests of others and the public interest and that is so even in the context of criminal proceedings. For example:

(1) In *Doorson v The Netherlands* (1996), no. 20524/92, §70, 26 March 1996 and *Van Mechelen v The Netherlands*, no. 21363/93; 21364/93; 21427/93;22056/93, §52-54, 23 April 1997 the ECtHR held that the principles of fair trial require that in appropriate cases the interests of the defence are balanced against those of witnesses or victims, and therefore that the use of statements made by anonymous witnesses to found a criminal conviction was not in principle incompatible with Art. 6.

(2) In *Jasper v United Kingdom*, no. 27052/95, §52, 16 February 2000 the ECtHR held that limitations on disclosure of relevant evidence could in principle be justified

on public interest immunity grounds in order to keep secret police methods of investigation of crime.

(3) In *Tinnelly & Sons Ltd and McElduff v United Kingdom, no. 20390/92; 21322/92,* §71-78, *10 July 1998* and *A v United Kingdom* at §§205-206, the ECtHR held that restrictions on the right to a fully adversarial procedure may in principle be permissible where strictly necessary to protect national security.

7.19 These limitations reflect the fact that there is a balance inherent in the whole of the Convention between the rights of the individual and the rights and interests of the community as a whole: see, eg, *Soering v United Kingdom*, no. 14038/88, §89, 19 January 1989.

7.20 That balance recognises that other rights and other vital interests may be in play. National security, which is not an end in itself but a necessary component in the protection of the public from serious threats and harm, is one important example. The Court has long recognised that the need to protect a State's citizens from risk of terrorist attack is one of the most pressing competing interests: see, for example, *Klass v Germany*, no. 5029/71, §48, 6 September 1978 and *Chahal v United Kingdom, no. 22414/93,* §79, 15 November 1996.

7.21 Thus, so far as civil proceedings are concerned, there is scope under the Convention for restrictions on the general position of full disclosure of relevant material when determining civil rights and obligations.

Principles governing permissible limitations on implied rights

7.22 It is of course acknowledged that the usual position is that fairness, even in civil proceedings, requires full disclosure of all information relevant to the issues being determined; and requires a reasoned judgment referring as necessary to all such relevant information. However, it is equally clear that that approach can be subject to limitations. Specifically national security considerations can, and in some circumstances must, impact on the specific ingredients of fairness. In practice such considerations will render it difficult, and on occasion impossible, to open up information relevant to the issues.

7.23 When assessing whether a particular limitation is permissible under Article 6, the approach of the Court has been constant. It asks two questions:

(1) Is the restriction "strictly necessary"? It must be directed to a proper social objective and go no further than is required to meet that objective; and

(2) Is the restriction "sufficiently counterbalanced" by the procedures in place?

(See *Tinnelly & Sons Ltd v United Kingdom*, no. 20390/92; 21322/92, §72, 10 July 1998 *Rowe and Davis v United Kingdom* at §61; *Botmeh and Alami v United Kingdom*, no. 15187/03, §37, 7 June 2007 *Kennedy v United Kingdom* at §180).

7.24 As to necessity, there is a clear and consistent line of Court jurisprudence recognising that the protection of national security interests (which exist in order to protect the rights and interests of the public, including in particular their safety) provides a legitimate basis on which material may have to be withheld: see eg *Leander v Sweden*, no. 9248/81, §49, §59 and §66, 26 March 1987, *Tinnelly & Sons v United Kingdom* at §76; *A v United Kingdom* at §§205-206 and §218 and *Kennedy v UK* at §§184-190.

7.25 In addition the Court has emphasised that the primary procedural safeguard is the scrutiny which can be provided by an independent court, fully appraised of all relevant material (see *Tinnelly & Sons Ltd & McElduff v United Kingdom* at §78 and see *Liu & Liu v Russia*, no. 29157/09, 26 July 2011 at §61 and §63[159]).

Kennedy v United Kingdom

7.26 In *Kennedy* the Court considered that scrutiny of relevant material by the IPT provided sufficient procedural safeguards against abuse.

[159] See also the similar cases of *Dağtekin v Turkey* (App. No. 70516/01) (13 December 2007) and *Gencer v Turkey* (App. No. 31881/02) (25 November 2008), both of which concerned the annulment on national security grounds of the applicants' right to farm land (which deprived them of their livelihoods). In those cases, the Court concluded that the applicants were deprived of sufficient procedural safeguards because the conclusions of the security investigation were not communicated to the domestic courts.

7.27 The Court noted the extensive jurisdiction of the IPT to examine any complaint of unlawful interception which included: the independence and impartiality of the IPT and the judicial experience of its members; the fact that the IPT had access to closed material and the power to order disclosure of relevant documents by those involved in the authorisation and execution of a warrant; and that the IPT's legal rulings were published: §167.

7.28 The Court held that the need to keep secret sensitive and confidential information justified the strong restrictions on disclosure of relevant information in proceedings before the IPT in the UK. Almost all of the relevant information considered and relied upon by the IPT was not disclosed to the applicant. The needs of national security precluded such a course. The Court assumed (without deciding) that Article 6(1) was engaged. Yet, the Court held that the IPT's procedures complied with the fairness requirement in Art. 6.

7.29 Critically, the Court found that the need to retain the secrecy of any surveillance measures was decisive in determining the extent of procedural safeguards, stating at §§186-187:

> "*At the outset, the Court emphasises that the proceedings related to secret surveillance measures and that there was therefore a need to keep secret sensitive and confidential information. In the Court's view, this consideration justifies restrictions in the IPT proceedings. The question is whether the restrictions, taken as a whole, were disproportionate or impaired the very essence of the applicant's right to a fair trial.*
>
> > *In respect of the rules limiting disclosure, the Court recalls that the entitlement to disclosure of relevant evidence is not an absolute right. The interests of national security or the need to keep secret methods of investigation of crime must be weighed against the general right to adversarial proceedings. … The Court further observes that documents submitted to the IPT in respect of a specific complaint, as well as details of any witnesses who have provided evidence, are likely to be highly sensitive, particularly when viewed in light of the Government's 'neither confirm nor*

deny' policy. The Court agrees with the Government that, in the circumstances, it was not possible to disclose redacted documents or to appoint special advocates as these measures would not have achieved the aim of preserving the secrecy of whether any interception had taken place."

7.30 Accordingly, the ECtHR concluded at §190 that:

"...the restrictions on the procedure before the IPT did not violate the applicant's right to a fair trial. In reaching this conclusion the Court emphasises the breadth of access to the IPT enjoyed by those complaining about interception within the United Kingdom and the absence of any evidential burden to be overcome in order to lodge an application with the IPT. In order to ensure the efficacy of the secret surveillance regime, and bearing in mind the importance of such measures to the fight against terrorism and serious crime the Court considers that the restrictions on the applicant's rights in the context of the proceedings before the IPT were both necessary and proportionate and did not impair the very essence of the applicant's Article 6 rights."

7.31 Consequently, despite the paucity of disclosure in open in that case, the Tribunal proceedings were nevertheless Art. 6(1) compliant.

The appointment of Counsel to the Tribunal (CTT)

7.32 In *Kennedy* the Court agreed with the Government that, in the circumstances of that case, it was not possible to appoint special advocates, as such a step could not have achieved the aim of preserving the secrecy of whether any interception had taken place (see §187).

7.33 However in the Liberty IPT proceedings (which involved general challenges to the regimes governing the intelligence sharing and s.8(4) regimes), CTT were appointed and, in practice, they performed an essentially similar function to special advocates (see §10 of the 5 December judgment). That included reviewing the CLOSED disclosure provided to the Tribunal to identify documents, parts of documents or gists that ought properly to be disclosed and making submissions to the IPT in

favour of disclosure as were in the interests of the claimants and open justice (see §10 of the 5 December judgment).

7.34 In a series of cases the Court has emphasised the role which can be played by special advocates as a safeguard where closed procedures are deployed: see *Chahal v United Kingdom*. no. 22414/93, 15 November 1996, at §144, *Jasper v United Kingdom* at §§36-38 and §55, *Al-Nashif v Bulgaria,* app. 50963/99, §§95-97, 20 June 2002, *A & others v United Kingdom at §*220 and *Othman (Abu Qatada) v United Kingdom*[160] at §§222-224. In *Othman* the Court emphasised the "rigorous scrutiny" which can be provided by special advocates, particularly where there are issues of a general nature which do not depend upon specific instructions from an individual claimant (see, in particular, §§223-224).

7.35 Consequently, the appointment of CTT in the IPT proceedings (acting effectively as special advocates) is a further important counterbalance to any compromise in the fairness of the proceedings due to the requirements of national security. As was the position in *Othman,* CTT can be particularly effective in IPT proceedings where the issues in the case do not require specific instructions from individuals (eg. about a positive national security case against them) and where eg. the central issue is the compatibility of the regime with ECHR standards. CTT is well-placed to make submissions in CLOSED to the IPT on the CLOSED disclosure provided to the IPT and its significance in terms of the lawfulness of the regimes.

Fairness of the IPT proceedings in Liberty

7.36 The Applicants have made a number of specific criticisms about the fairness of the IPT proceedings, each of which has been considered in turn below. Overall it is submitted that the IPT proceedings were patently fair given the following particular features of the proceedings:

(1) The applicants did not have to overcome any evidential burden to apply to the IPT.

(2) There was scrutiny of <u>all</u> the relevant material, open and closed, by the

[160] Application No. 8139/09 17 January 2012, 32 B.H.R.C. 62

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 concerns.

(4) The Tribunal appointed Counsel to the Tribunal (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).

7.37 As to the specific complaints raised by the Applicants, **first** it is said 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. This is addressed at §§134-135 of the IPT's 5 December judgment. As is evident from that extract from the judgment:

(1) Liberty only sought to raise, at a very late stage of the IPT proceedings (in written submissions dated 17 November 2014), the issue whether there was adequate provision under Art. 10 ECHR for dealing with confidential information in the context of NGO activities ('NGO confidence');

(2) The issue of NGO confidence was not raised when the legal issues were agreed between all parties on 14 February 2014, some 5 months before the open legal issues hearing in July 2014;

(3) The written arguments addressed at the July 2014 hearing had not raised any separate issue under Art. 10 ECHR in respect of NGO confidence.

(4) Liberty had been given ample opportunity to raise the issue, but had not done so.

(5) The IPT concluded that it was far too late (in November 2014) to be seeking to raise the issue, particularly in circumstances where it was being suggested that further disclosure and "considerable" further argument would be necessary to incorporate it into the proceedings at that stage.

7.38 In those circumstances, the IPT cannot be criticised for declining to address this additional issue at the hearing and thereby not pursuing any separate issue of disclosure which arose in relation to it.

7.39 **Secondly**, the Applicants state that the IPT took the position that it had no power, in any event, to require the intelligence services to disclose such evidence. But there is no finding in the IPT's judgments to the effect that it had no power to require the intelligence services to disclose such evidence. That was not a live issue in the proceedings, in circumstances where the Intelligence Agencies had agreed to make all of the disclosure which the IPT had suggested. As stated at §10 if the IPT judgment dated 5 December:

> *"...As will be seen, in the context of a closed hearing there were matters derived from the evidence in the closed hearing which the Respondents were prepared to consent to disclose, and there were no matters which the Tribunal considered should be disclosed which the Respondents declined to disclose. Written submissions by the parties and a further closed and open hearing then followed, and some further matters were disclosed voluntarily by the Respondents."*(emphasis added)

7.40 It is therefore wrong to suggest that the IPT took the position that it had no power to order disclosure in the proceedings; that issue did not arise in the proceedings given that the Respondents were content to disclose that which the Tribunal suggested should be disclosed.

7.41 **Thirdly** the applicants assert that the IPT wrongly held a closed hearing on whether the relevant framework governing the intelligence services' interception and receipt of material of foreign intelligence agencies was in accordance with the law. But 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 and the public interest. 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:

"After the five day public hearing, we held a one day closed hearing to consider certain matters which were, in the considered judgment of the Respondents, too confidential and sensitive for discussion in open court in the interests of preserving national security, and in accordance with our jurisdiction to hold such a closed hearing pursuant to Rule 9 of the Investigatory Powers Tribunal Rules 2000. As will appear, we considered in particular the arrangements,...described during the public hearing as "below the waterline", regulating the conduct and practice of the Intelligence Services, in order to consider (i) their adequacy and (ii) whether any of them could and should be publicly disclosed in order to comply with the requirements of Articles 8 and 10 of the Convention as interpreted by the ECtHR, to which we will refer further below.

...[The IPT] has access to all secret information, and can adjourn into closed hearing in order to assess whether the arrangements (a) do indeed exist as asserted by Mr Farr, (b) are adequate to do the job of giving the individual "adequate protection against arbitrary interference.

[The IPT] has, and takes, the opportunity, with the benefit of full argument, to probe fully whether matters disclosed to it in closed hearing, pursuant to the Respondents' obligation to do so pursuant to s.68(6) of RIPA, can and should be disclosed in open and thereby publicised."

7.42 Consequently the IPT's approach of considering the internal arrangements in closed enabled the IPT to consider whether more could be said about them in open and, in fact, further disclosures were made in respect of such arrangements, as is evident from §10, §46, §47 and §126 of the 5 December judgment.

7.43 In addition CTT were appointed in the proceedings and made submissions from the perspective of the claimants in the closed hearing, both on the issue of disclosure and in order to ensure that all relevant arguments on the facts and the law were put to the tribunal. CTT summarised their functions in terms which largely accorded with

the claimants' submissions on what those functions should be[161]; and the IPT specifically adopted that summary[162]. The summary stated, *inter alia*:

> *"there is a broad measure of agreement between the Claimants and the Respondents that counsel to the Tribunal can best assist the Tribunal by performing the following roles: (i) identifying documents, parts of documents or gists that ought properly to be disclosed; (ii) making such submissions to the Tribunal in favour of disclosure as are in the interests of the Claimants and open justice; and (iii) ensuring that all the relevant arguments on the facts and the law are put before the Tribunal. In relation to (iii), the Tribunal will expect its counsel to make submissions from the perspective of the Claimants' interests (since the Respondents will be able to make their own submissions). If the Tribunal decides to receive closed oral evidence from one or more of the Respondent's witnesses, it may also direct its counsel to cross-examine them. In practice, the roles performed by counsel to the Tribunal at this stage of the current proceedings will be similar to those performed by a Special Advocate in closed material proceedings."* (Emphasis added)

7.44 In those circumstances, the IPT was plainly right when it rejected the contention that the holding of a closed hearing had been unfair. At §50(ii) of the 5 December judgment it stated:

> "*We do not accept that the holding of a closed hearing, as we have carried it out, is unfair. It accords with the statutory procedure, and facilitates the process referred to in paragraphs 45 and 46 above. This enables a combination of open and closed hearings which both gives the fullest and most transparent opportunity for hearing full arguments inter parties on hypothetical or actual facts, with as much as possible heard in public, and preserves the public interest and national security.*"

7.45 Given the Court's conclusions in *Kennedy*, there was clearly no breach of Art. 6 in the approach taken by the IPT.

7.46 **Fourthly** it is said that the IPT refused to hear and decide one of the preliminary issues that was agreed between the parties, namely whether the Respondents'

[161] See the attached submissions of CTT, [***See Annex 62***]
[162] See the IPT's email of 12 September 2014, [***See Annex 63***]

'neither confirm nor deny' ('NCND') policy in relation to the existence of particular interception programmes, was justified. However, as is evident from §13 of the judgment dated 5 December, that issue was, by agreement between the parties, not decided by the IPT:

> *"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*[163]*…* (emphasis added)

In those circumstances the Applicants cannot now complain that this issue was

[163] Those open paragraphs of the Response stated:
"5. Secrecy is essential to the necessarily covert work and operational effectiveness of the Intelligence Services, whose primary function is to protect national security. See e.g Attorney General v. Guardian Newspapers Ltd (No.2)[1990] 1 AC 109, per Lord Griffiths at 269F.
6. As a result, the mere fact that the Intelligence Services are carrying out an investigation or operation in relation to, say, a terrorist group, or hold information on a suspected terrorist, will itself be sensitive. If, for example, a hostile individual or group were to become aware that they were the subject of interest by the Intelligence Services, they could not only take steps to thwart any (covert) investigation or operation but also attempt to discover, and perhaps publicly reveal, the methods used by the Intelligence Services or the identities of the officers or agents involved. Conversely, if a hostile individual or group were to become aware that they were not the subject of Intelligence Service interest, they would then know that they could engage or continue to engage in their undesirable activities with increased vigour and increased confidence that they will not be detected.
7. In addition, an appropriate degree of secrecy must be maintained as regards the intelligence-gathering capabilities and techniques of the Intelligence Services (and any gaps in or limits to those capabilities and techniques). If hostile individuals or groups acquire detailed information on such matters then they will be able to adapt their conduct to avoid, or at least minimise, the risk that the Intelligence Services will be able successfully to deploy those capabilities and techniques against them.
8. It has thus been the policy of successive UK Governments to neither confirm nor deny whether they are monitoring the activities of a particular group or individual, or hold information on a particular group or individual, or have had contact with a particular individual. Similarly, the long-standing policy of the UK Government is to neither confirm nor deny the truth of claims about the operational activities of the Intelligence Services, including their intelligence-gathering capabilities and techniques.
9. Further, the "neither confirm nor deny" principle would be rendered nugatory, and national security thereby seriously damaged, if every time that sensitive information were disclosed without authority (i.e. "leaked"), or it was alleged that there had been such unauthorised disclosure of such information, the UK Government were then obliged to confirm or deny the veracity of the information in question.
10. It has thus been the policy of successive Governments to adopt a neither confirm nor deny stance in relation to any information derived from any alleged leak regarding the activities or operations of the Intelligence Services insofar as that information has not been separately confirmed by an official statement by the UK Government. That long-standing policy is applied in this Open Response."
Because this hearing has been held on the basis of agreed assumed facts, it has not been necessary to address this policy or its consequences."

not determined by the IPT.

7.47 Further, and 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 *Klass* at §58, *Weber* at §135 and *Segerstedt-Wiberg v Sweden*, judgment 6 June 2006 at §102. 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.

7.48 In those circumstances and given that the IPT gave specific consideration to what information could be disclosed in the proceedings, assisted, as it was in closed, by CTT (see §7 and §10 of the 5 December judgment), there was no failure to consider an issue which could have impacted on the fairness of the proceedings.

7.49 **Fifthly** the Applicants complain that, in finding that the regime was in accordance with the law, it placed significant reliance on secret arrangements which were not disclosed to the Applicants and on which the Government were permitted to make submissions during closed proceedings. The Government repeat the submissions at §§7.41-7.45 above. In short, recourse to closed material was strictly necessary given the national security concerns which arose, but any inroads into the fairness of the proceedings were sufficiently counterbalanced by the independent scrutiny provided by the IPT, with the assistance of CTT in the proceedings.

7.50 **Finally** it is said that the IPT took no steps to ensure that the Applicants were effectively represented in closed proceedings. For the reasons already set out above, this has no merit. CTT was appointed and did represent the Applicants' interests in the closed proceedings, as referred to at §10 of the IPT's 5 December judgment, and as set out at §§7.32-7.35 above.

8 QUESTION 6. ARTICLE 14 OF THE CONVENTION

Whether there has been a violation of Article 14 taken together with Article 8

and/or Article 10 on account of the fact that the safeguards set out in s.16 of RIPA 2000 grants additional safeguards to people known to be in the British Islands?

8.1 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"*[164] 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.

8.2 The true position is as follows:

(1) The operation of the s.8(4) Regime does not mean that persons outside the United Kingdom are disproportionately likely to have their private communications intercepted. The Applicants' case is factually incorrect.
(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. The Secretary of State must certify that it is necessary to examine intercepted material by reference to a factor referable to such a person. To that extent, persons are treated differently on the basis of current location.
(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?

8.3 The operation of the s. 8(4) Regime does not have the effect of making persons outside the British Islands more liable to have their communications intercepted, than persons within the British Islands. "*External communications*" include those which are sent from outside the British Islands, to a recipient in the British Islands; or

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

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.

8.4 The sole respect in which persons may be treated differently by reason of current location under the s. 8(4) Regime is that at the selection stage, limitations are imposed on the extent to which intercepted material can be selected to be read, looked at or listened to according to a factor which is referable to an individual who is known to be for the time being in the British Islands (for example, by reference to a UK landline telephone number). Before such a course may be taken, the Secretary of State must certify that it is necessary under s.16 RIPA.

8.5 The Applicants contend that this difference in treatment on the basis of current location amounts to a relevant difference in treatment for the purposes of Article 14, saying that it amounts to indirect discrimination on grounds of nationality. That contention is contrary to the ECtHR's case law, which 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[165].

8.6 In any event, if, contrary to the above, that difference in current location is a relevant difference in treatment, then it is clearly justified.

Justification

8.7 In assessing whether and to what extent differences in otherwise similar situations justify differential treatment, the ECtHR allows States a margin of appreciation,

[165] The applicant in *Magee* was arrested in Northern Ireland on suspicion of terrorism. He complained that his treatment was contrary to Art 14 because suspects arrested and detained in England and Wales under prevention of terrorism legislation could inter alia have access to a lawyer immediately; and that was not the case in Northern Ireland. The Court said that any difference in treatment was *"not to be explained in terms of personal characteristics, such as national origin or association with a national minority, but on the geographical location where the individual is arrested and detained"* and that the difference did not amount to discriminatory treatment within the meaning of Art 14.

which varies according both to the ground for differential treatment, and the subject matter at issue. Thus, 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. Thus, to the extent that Art 14 is engaged at all, the present circumstances 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.

8.8 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.

8.9 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. 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.

8.10 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 <u>should be relatively rare</u>. 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.

8.11 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.

8.12 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.

8.13 **First,** that analysis 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 Cairo. In general, the Government should be able to investigate an identifiable Birmingham-based individual without the need to examine data obtained under a s. 8(4) warrant at all; not so for the individual in Cairo.

8.14 **Secondly,** it assumes that the Intelligence Agencies are likely to have the same base of knowledge from which to identify the communications of a person in Cairo, 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 Cairo 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 for the purpose of identifying communications from or to the individual in Cairo would have to be certified by the Secretary of State, because any such factors would be "referable" to him.

8.15 **Thirdly,** 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.

8.16 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 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.

Anna McLeod

Anna McLeod

18 April 2016 (Agent of the Government of the United Kingdom)