DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix AA

IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, INC. Plaintiff, v. NATIONAL SECURITY AGENCY, et al., Defendants.	Civil Action No. 1:15-cv-00662-TSE Hon. T.S. Ellis, III

WIKIMEDIA FOUNDATION, INC.'S SECOND AMENDED AND SUPPLEMENTAL RESPONSES AND OBJECTIONS TO NATIONAL SECURITY AGENCY'S FIRST SET OF INTERROGATORIES

PROPOUNDING PARTY: **NATIONAL SECURITY AGENCY**

RESPONDING PARTY: **WIKIMEDIA FOUNDATION, INC.**

SET NUMBER: **ONE**

Pursuant to Federal Rule of Civil Procedure 33, Plaintiff Wikimedia Foundation, Inc. ("Plaintiff" or "Wikimedia") amends and supplements its responses as follows to Defendant National Security Agency's ("Defendant" or "NSA") (collectively with Plaintiff, the "Parties") First Set of Interrogatories (the "Interrogatories"):

I. GENERAL RESPONSES.

1. Plaintiff's response to Defendant's Interrogatories is made to the best of Plaintiff's present knowledge, information, and belief. Discovery in this action is ongoing, and Plaintiff's responses may be substantially altered by further investigation, including further review of Plaintiff's own documents, as well as the review of documents produced by Defendant. Said response is at all times subject to such additional or different information that discovery or

further investigation may disclose and, while based on the present state of Plaintiff's recollection, is subject to such refreshing of recollection, and such additional knowledge of facts, as may result from Plaintiff's further discovery or investigation.

2. Plaintiff reserves the right to make any use of, or to introduce at any hearing and at trial, information and/or documents responsive to Defendant's Interrogatories but discovered subsequent to the date of this response, including, but not limited to, any such information or documents obtained in discovery herein.

3. To the extent that Plaintiff responds to Defendant's Interrogatories by stating that Plaintiff will provide information and/or documents that Plaintiff deems to embody material that is private, business confidential, proprietary, trade secret, or otherwise protected from disclosure pursuant to Federal Rule of Civil Procedure 26(c)(7), Federal Rule of Evidence 501, or other applicable law, Plaintiff will do so only pursuant to the Parties' Stipulated Protective Order (ECF No. 120).

4. Plaintiff reserves all objections or other questions as to the competency, relevance, materiality, privilege, or admissibility as evidence in any subsequent proceeding in or trial of this or any other action for any purpose whatsoever of Plaintiff's responses herein and any document or thing identified or provided in response to Defendant's Interrogatories.

5. Plaintiff's responses will be subject to and limited by any agreements the Parties reach concerning the scope of discovery.

6. Plaintiff reserves the right to object on any ground at any time to such other or supplemental interrogatories as Defendant may at any time propound involving or relating to the subject matter of these Interrogatories.

II. GENERAL OBJECTIONS.

Plaintiff makes the following general objections, whether or not separately set forth in response to each Interrogatory, to each instruction, definition, and Interrogatory made in Defendant's Interrogatories:

1. Plaintiff objects to the Interrogatories in their entirety insofar as any such instruction, definition, or Interrogatory seeks information or production of documents protected by the attorney-client privilege or the work product doctrine. Fed. R. Civ. Proc. 26(b)(1). Such information or documents shall not be provided in response to Defendant's Interrogatories and any inadvertent disclosure or production thereof shall not be deemed a waiver of any privilege with respect to such information or documents or of any work product immunity which may attach thereto. Fed. R. Civ. Proc. 26(b)(5)(B).

2. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks identification of documents, witnesses, or information that Defendant has withheld from Plaintiff. Fed. R. Civ. Proc. 26(b)(1), (2).

3. Plaintiff objects to the Interrogatories in their entirety to the extent any such Interrogatory requires Plaintiff to identify potentially thousands of pages of documents, not all of which have been or can be located and reviewed by counsel within the time period allowed for this response or within a reasonable time. Accordingly, said Interrogatories would subject Plaintiff to unreasonable and undue annoyance, oppression, burden and expense.

4. Plaintiff objects to any Interrogatories that exceed the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and ordered by the Court.

5. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks information that is available through or from public

sources or records, or that are otherwise equally available to Defendant, on the ground that such instructions, definitions, and/or Interrogatories unreasonably subject Plaintiff to undue annoyance, oppression, burden, and expense. Fed. R. Civ. Proc. 26(b)(1), (2).

6. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory purport to impose obligations that are greater or more burdensome than or contradict those imposed by the applicable Federal and local rules. *See* Fed. R. Civ. Proc. 26, 33.

7. Plaintiff objects to the Interrogatories in their entirety as the Interrogatories contain more than the "25 written interrogatories, including all discrete subparts," permitted by the Federal Rules of Civil Procedure, Rule 33(a)(1), and Defendant has not sought leave to serve additional interrogatories.

8. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks documents or information no longer in existence or not currently in Plaintiff's possession, custody, or control, or to the extent they refer to persons, entities, or events not known to Plaintiff or controlled by Plaintiff, on the grounds that such definitions or Interrogatories are overly broad, seek to require more of Plaintiff than any obligation imposed by law, would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense, and would seek to impose upon Plaintiff an obligation to investigate, discover, or produce information or materials from third parties or otherwise that are accessible to Defendant or readily obtainable from public or other sources. Fed. R. Civ. Proc. 26(b)(1), (2).

9. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks information or production of documents protected

from disclosure by any right to privacy or any other applicable privilege or protection, including the right to confidentiality or privacy of third parties, any right of confidentiality provided for by Plaintiff's contracts or agreements with such third parties, or by Plaintiff's obligations under applicable law or contract to protect such confidential information. Plaintiff reserves the right to withhold any responsive information or documents governed by a third-party confidentiality agreement until such time as the appropriate notice can be given or the appropriate permissions can be obtained. Plaintiff also objects generally to all instructions, definitions, or Interrogatories to the extent they seek disclosure of trade secrets and other confidential research or analyses, development, or commercial information of Plaintiff or any third party.

10. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory is overbroad and unduly burdensome, particularly to the extent they seek "all," "each," or "any" documents, witnesses or facts relating to various subject matters. Fed. R. Civ. Proc. 26(b)(1), (2). To the extent Plaintiff responds to such Interrogatories, Plaintiff will use reasonable diligence to identify responsive documents, witnesses or facts in its possession, custody, or control, based on its present knowledge, information, and belief.

11. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks expert discovery prematurely.

12. Plaintiff objects to any contention Interrogatories in their entirety as premature. Plaintiff will provide its response prior to the close of fact discovery.

13. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory purports to require Plaintiff to restore and/or search data sources that are not reasonably accessible on the grounds that such definitions and Interrogatories would subject Plaintiff to undue burden and expense. Fed. R. Civ. Proc. 26(b)(1), (2).

III. DEFINITIONAL OBJECTIONS.

1. Plaintiff objects to definition number one (1) to the extent it defines "Plaintiff" and "Wikimedia" to include Plaintiff's "parent, subsidiary, and affiliated organizations, and all persons acting on their behalf, including officials, agents, employees, attorneys, and consultants." Said definition is overly broad, seeks irrelevant information not calculated to lead to the discovery of admissible evidence, seeks information outside of Plaintiff's possession, custody, or control, and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden and expense. Said definition is also vague and ambiguous in that it cannot be determined what is meant by the terms "affiliated organizations" and "all persons acting on their behalf." Plaintiff shall construe "Plaintiff" and "Wikimedia" to mean Wikimedia, and its present officers, directors, agents, and employees.

2. Plaintiff objects to definition number four (4) and to each Interrogatory that purports to require Plaintiff to "state the basis of," "stating the basis of," "state on what basis," or otherwise "state with particularity" or "identify" "all" facts, documents, or persons whose testimony support or dispute any given factual assertion, on the ground that any response thereto would require subjective judgment on the part of Plaintiff and its attorneys, and would further require disclosure of a conclusion or opinion of counsel in violation of the attorney work product doctrine and/or attorney-client privilege. Plaintiff further objects that this definition and all requests to identify documents in the Interrogatories are premature at this early stage of the litigation, would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense, and would impose an obligation to provide information greater than that required by the Federal Rules of Civil Procedure.

3. Plaintiff objects to definition number five (5) as unduly burdensome in that it

purports to require Plaintiff to "identify" each "natural person" by providing information including "her most current home and business addresses, telephone numbers, and e-mail addresses, the name of her current employer, and her title."

4. Plaintiff objects to definition number six (6) as unduly burdensome in that it purports to require Plaintiff to "identify" an "entity that is not a natural person" by providing information including "its telephone number and e-mail address, and the full names, business addresses, telephone numbers, and e-mail addresses of both its chief executive officer and an agent designated by it to receive service of process."

5. Plaintiff objects to definition number seven (7) as unduly burdensome in that it purports to require Plaintiff to "identify" documents by providing "(a) the nature of the document (*i.e*, letter, memorandum, spreadsheet, database, etc.); (b) its date; (c) its author(s) (including title(s) or position(s)); (d) its recipient(s) (including title(s) or position(s)); (e) its number of pages or size; and (f) its subject matter," or by providing information in accordance with Defendant's "Specifications for Production of ESI and Digitized ('Scanned') Images attached to Defendant National Security Agency's First Set of Requests for Production." Plaintiff further objects that this definition and all requests to identify documents in the Interrogatories are premature at this early stage of the litigation, would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense, and would impose an obligation to provide information greater than that required by the Federal Rules of Civil Procedure.

IV. INSTRUCTIONAL OBJECTIONS

1. Plaintiff objects to instruction number one (1) to the extent it purports to request "knowledge or information" from Wikimedia's "parent, subsidiary, or affiliated organizations, and their officials, agents, employees, attorneys, consultants, and any other person acting on their

behalf." Said request is overly broad, seeks irrelevant information not calculated to lead to the discovery of admissible evidence, seeks information outside Plaintiff's possession, custody, or control, and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden and expense. Moreover, said request is vague and ambiguous in that it cannot be determined what is meant by the term "affiliated organizations" and "any other person acting on their behalf." Where an Interrogatory requests knowledge or information of Plaintiff, Plaintiff shall construe such request to mean knowledge or information from Wikimedia, and its present officers, directors, agents, and employees.

2. Plaintiff objects to instruction number three (3) as unduly burdensome and imposing an obligation to provide information greater than that required by the Federal Rules of Civil Procedure to the extent it purports to require Plaintiff to "identify each person known by Plaintiff to have such knowledge, and in each instance where Plaintiff avers insufficient knowledge or information as a grounds for not providing information or for providing only a portion of the information requested, set forth a description of the efforts made to locate information needed to answer the interrogatory."

3. Plaintiff objects to instruction number four (4) to the extent it seeks to require it to identify anything other than the specific claim of privilege or work product being made and the basis for such claim, and to the extent it seeks to require any information not specified in Discovery Guideline 10, on the grounds that the additional information sought by Defendant would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense, and constitutes information protected from discovery by privilege and as work product. Plaintiff is willing to discuss acceptable reciprocal obligations for disclosure of information withheld on the basis of attorney-client privilege or attorney work-product.

4. Plaintiff objects to instruction number five (5) to the extent it defines "the time period for which each interrogatory seeks a response" as "the period from July 10, 2008 (the date of enactment of the FISA Amendments Act of 2008, Pub. L. 110-261, 121 Stat. 522) until the date of Plaintiff's response." This definition is overly broad, seeks irrelevant information not calculated to lead to the discovery of admissible evidence, and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense. Where appropriate, Plaintiff has defined the specific time period encompassed by specific responses.

5. Plaintiff objects to instruction number six (6) that the Interrogatories are continuing, to the extent said instruction seeks unilaterally to impose an obligation to provide supplemental information greater than that required by Federal Rule of Civil Procedure 26(e) and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense. Plaintiff will comply with the requirements of the Federal Rules of Civil Procedure and is willing to discuss mutually acceptable reciprocal obligations for continuing discovery.

V. SPECIFIC OBJECTIONS AND RESPONSES TO INTERROGATORIES.

Without waiving or limiting in any manner any of the foregoing General Objections, Definitional Objections, or Instructional Objections, but rather incorporating them into each of the following responses to the extent applicable, Plaintiff responds to the specific Interrogatories in Defendant's Interrogatories as follows:

INTERROGATORY NO. 2:

Unless Plaintiff's response to Interrogatory No. 1, above, is an unequivocal "no," then please state the basis of Plaintiff's contention that NSA Upstream surveillance involves the interception, copying, and review of all or substantially all international Internet text-based communications, including, but not limited to, the contentions that "Upstream surveillance is

intended to enable the comprehensive monitoring of international internet traffic," see Amended Complaint ¶ 48; that "the NSA is temporarily copying and then sifting through the contents of what is apparently most e mails and other text-based communications that cross the border," see id. ¶ 69; that "it would be difficult to systematically search the contents of the communications without first gathering nearly all cross-border text-based data," see Pl.'s Opp. to Defs.' MTD at 18-19; and that the U.S. Government "has acknowledged … that the NSA … examines the full contents of essentially everyone's communications to determine whether they include references to the NSA's search terms," *see id.* at 10.

RESPONSE TO INTERROGATORY NO. 2:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is a contention Interrogatory that is premature at this stage in the litigation. Plaintiff further submits that these matters may be the subject of expert testimony, as to which Plaintiff will provide discovery at the appropriate time.

Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery. Plaintiff additionally objects that this Interrogatory is improperly compound in that it contains multiple subparts.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

The bases for Plaintiff's contention include the following:

- Basic principles underlying how Internet communications are transmitted and how surveillance on a packet-switched network operates.

- Privacy & Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* (2014) ("PCLOB Report"), including pages 7–10, 12–

13, 22, 30–41 & n.157, 79, 111 n.476, 120–22, 125, 143, and official government sources concerning Upstream surveillance cited therein.

- [*Redacted*], No. [Redacted], 2011 WL 10945618 (FISC Oct. 3, 2011)
- 50 U.S.C. §§ 1801, 1881a.
- David S. Kris & J. Douglas Wilson, *National Security Investigations and Prosecutions* § 17.5 (July 2015)
- Julia Angwin & Jeff Larson, *New Snowden Documents Reveal Secret Memos Expanding Spying*, ProPublica (June 4, 2015) (and associated documents)
- Julia Angwin et al., *AT&T Helped U.S. Spy on Internet on Vast Scale*, N.Y. Times, Aug. 15, 2015 (and associated documents)
- Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents)
- Jeff Larson et al., *A Trail of Evidence Leading to AT&T's Partnership with the NSA*, ProPublica, Aug. 15, 2015 (and associated documents)
- PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 26:15–18 (Mar. 19, 2014) (statement of Robert Litt, General Counsel, ODNI)
- Charlie Savage, *Power Wars* (2015)

Additionally, Plaintiff's contention is based on the principles of Internet communication and the technical necessities of the inspection of Internet communications in transit.

For example, Internet communications in transit are split into packets. Where an eavesdropper is attempting to determine whether the contents of a particular communication in transit on the Internet contain a particular piece of information, the eavesdropper generally must

reassemble the packets constituting the communication and then scan the reassembled communication. Reassembling Internet packets requires the temporary copying (or "caching") of those packets until all packets needed for the reassembly have arrived.

Additionally, Upstream surveillance involves the retention of communications that contain targeted selectors. To retain a communication in transit, an eavesdropper must copy and reassemble the packets constituting the communication. But because an eavesdropper cannot know in advance which packets in transit are part of a communication containing a targeted selector, the eavesdropper must create a temporary copy of all packets that might be a part of such a communication.

The fact that all or substantially all international Internet text-based communications are subject to Upstream surveillance follows necessarily from the information the government has officially disclosed, and it is corroborated by independent news reports. For Upstream surveillance to serve the purposes the government has said it serves, the NSA must be comprehensively monitoring text-based communications originating or terminating in the United States. This is the only way for the NSA to reliably obtain communications to, from, and about its thousands of targets around the world, because those communications travel along paths in and out of the country that are unpredictable and change over time. Moreover, the structure of the Internet backbone facilitates such comprehensive surveillance. Because international communications are channeled through a small number of Internet chokepoints—and because the NSA's own documents show that it is conducting Upstream surveillance at many of those chokepoints—it is straightforward for the government to conduct the comprehensive surveillance necessary for Upstream to function as described.

The government's descriptions of Upstream surveillance make clear that the government

is interested in obtaining, with a high degree of confidence, all international communications to, from, and about its targets. For example, the Privacy and Civil Liberties Oversight Board has described the use of Upstream surveillance to collect "about" communications as "an inevitable byproduct of the government's efforts to *comprehensively* acquire communications that are sent to or from its targets." PCLOB Report 10 (emphasis added). And it has said about Upstream surveillance more generally that this method's "success . . . depends on collection devices that can reliably acquire data packets associated with the proper communications." *Id.* at 143 (emphasis added).

Because the routing of Internet traffic is unpredictable, however, the government can only "comprehensively" and "reliably" obtain communications to, from, and about its thousands of targets by conducting its surveillance on the different routes by which Internet communications enter and leave the country, and by examining substantially all international communications that travel those various routes.

The path that an Internet communication takes is inherently unpredictable. Internet communications are routed around the globe based on a complex set of rules and relationships that are applied dynamically, based on network conditions at any given moment. These network conditions change frequently, and so one cannot know in advance which path a particular communication will travel. Indeed, even the communications between two individuals in a single conversation (such as an Internet chat or email exchange) may take entirely different routes across the Internet backbone, even though the end-points are the same. For example, if an NSA target is having an Internet chat conversation with someone in the United States, the communications *from* the target will frequently follow a different path than those *to* the target. And, of course, a target's location may vary over time. For all these reasons, a target's

communications may traverse one Internet circuit at one moment, but a different one later.

The fact that the NSA had, at last public count, 106,469 surveillance targets (some of which are groups with perhaps hundreds or even thousands of members) only reinforces the conclusion that Upstream surveillance of international text-based communications must be comprehensive. *See* ODNI, Statistical Transparency Report Regarding the Use of National Security Authorities for Calendar Year 2016 (Apr. 2017), https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2016. The communications of so many targets scattered around the world will travel many different routes across the Internet backbone, based on the locations of those various targets, their individual movements over time, and changes in network conditions. These communications will be intermingled with those of the general population in the flow of Internet traffic. An intelligence agency that seeks to reliably intercept communications to, from, or about its targets, could do so only by searching substantially all text-based communications entering or leaving the country.

This allegation is based on the government's official disclosures and on necessary inferences from those disclosures, but it is also corroborated by news accounts. A *New York Times* report from August 2013 states, based on a review of NSA documents and interviews with senior intelligence officials, that "the N.S.A. is temporarily copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border." Charlie Savage, *N.S.A. Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013, http://nyti.ms/1E1nlsi. The same *New York Times* report also explains why the NSA's Upstream surveillance is so far-reaching:

> "Computer scientists said that it would be difficult to systematically search the contents of the communications without first gathering nearly all cross-border text-based data;

> fiber-optic networks work by breaking messages into tiny packets that flow at the speed of light over different pathways to their shared destination, so they would need to be captured and reassembled."

Id.; see also Charlie Savage, *Power Wars* 207–11 (2015).

Not only does the NSA have an overriding incentive to copy and review substantially all international Internet communications, but the Internet backbone is structured in a way that enables it to do so.

The Internet backbone funnels almost all Internet communications entering and leaving the country through a limited number of chokepoints. The Internet backbone includes a relatively small number of international submarine cables (and a limited number of terrestrial cables) that transport Internet traffic into and out of the United States. Because there are relatively few high-capacity cables carrying international Internet communications, there are correspondingly few chokepoints—*i.e.*, junctions through which all international Internet communications must pass en route to their destinations. By installing its surveillance equipment at the small number of backbone chokepoints, the NSA is able to monitor substantially all text-based communications entering or leaving the United States. And the government has acknowledged that it conducts Upstream surveillance at international links and on the Internet backbone. [*Redacted*], 2011 WL 10945618, at *15; PCLOB Report 36–37.

NSA documents published in the press show that the NSA has installed surveillance equipment at many major chokepoints on the Internet backbone. One of these NSA documents states that the NSA has established interception capabilities on "many of the chokepoints operated by U.S. providers through which international communications enter and leave the United States." *See* Plaintiff's First Amended Complaint ¶ 69. Another shows that just one of

those participating providers has facilitated Upstream surveillance at seven major international chokepoints in the United States. *Id.* ¶ 68. Additional reporting states that the NSA has installed surveillance equipment in at least 17 "internet hubs" operated by another major U.S. telecommunications provider. Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents).

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 2:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement as discovery in this case continues, Plaintiff supplements its response as follows:

The bases for Plaintiff's contention also include the following: Glenn Greenwald, *No Place to Hide* (2014).

The fact that the NSA had, at last public count, 106,469 surveillance targets (some of which are groups with perhaps hundreds or even thousands of members) only reinforces the conclusion that Upstream surveillance of international text-based communications must be comprehensive. *See* ODNI, Statistical Transparency Report Regarding the Use of National Security Authorities for Calendar Year 2016 (Apr. 2017), https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2016; *see generally* ODNI Statistical Transparency Reports Regarding the Use of National Security Authorities.

SECOND SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 2:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement as discovery in this case continues, Plaintiff supplements its response as follows:

The bases for Plaintiff's contention also include the following:

- PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (Mar. 19, 2014)
- PCLOB, Public Hearing Regarding Consideration of Recommendations for Change: The Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act (Nov. 4, 2013)
- June 1, 2011 FISC submission
- July 15, 2015 FISC submission (2015 Summary of Notable Section 702 Requirements)
- June 28, 2011 FISC submission
- August 16, 2011 FISC submission
- November 15, 2011 FISC submission (Government's Responses to FISC Questions Re: Amended 2011 Section 702 Certifications)
- FISC Opinion (Sept. 25, 2012)
- FISC Opinion (Apr. 26, 2017)
- NSA Section 702 Targeting Procedures
- NSA Section 702 Minimization Procedures
- PCLOB, Recommendations Assessment Reports
- Executive Office of the President of the United States, The Comprehensive National Cybersecurity Initiative
- U.S. Dep't of Homeland Security, Privacy Impact Assessment for the Initiative Three Exercise (Mar. 18, 2010)

- OLC, Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (Einstein 2.0) to Protect Unclassified Computer Networks in the Executive Branch (Jan. 9, 2009)
- U.S. Dep't of Homeland Security, Privacy Impact Assessment for Einstein 3 – Accelerated (E3A) (Apr. 19, 2013)
- U.S. Dep't of Homeland Security, Privacy Impact Assessment for Einstein 2 (May 19, 2008)

INTERROGATORY NO. 6:

For each category of Wikimedia international, text-based, Internet communications identified in response to Interrogatory No. 3, above, that Plaintiff contends is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, please identify each foreign country to or from which such Wikimedia communications were sent in the past 24 months.

RESPONSE TO INTERROGATORY NO. 6:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is overbroad, unduly burdensome and seeks information that is not reasonably calculated to lead to the discovery of admissible evidence. Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, see ECF No. 116 at 4, and as ordered by the Court.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

(1) Wikimedia communications with its community members. Between April 23,

2017 and December 31, 2017, Wikimedia's U.S. servers received HTTPS requests from, and transmitted HTTPS responses to, users in at least 242 non-U.S. countries, territories and regions. This figure is an estimate that was derived using MaxMind geolocation data to determine the country associated with the client IP of each HTTPS request transmitted to Wikimedia's servers in the United States.

(2) Wikimedia's internal log communications. Every time Wikimedia receives an HTTPS request from a person accessing a Wikimedia Project webpage, it creates a corresponding log entry. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between January 1, 2015 and December 12, 2017, Wikimedia's office network router located in the United States sent Internet communications to at least approximately 221 non-U.S. countries, territories and regions.

This figure represents Internet outbound communications sent via the following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

This figure includes communications sent through Wikimedia's Virtual Private Network (VPN).

This figure does not account for the significant number of Internet communications by Wikimedia staff and contractors located internationally, who did not communicate using Wikimedia's Virtual Private Network, but who routinely communicate with Wikimedia staff located at the U.S. headquarters. Between January 1, 2015 and December 22, 2017, Wikimedia engaged over 80 contractors, located across more than 30 different countries.

The results of these analyses will be produced to Defendants. An anonymized list of

Plaintiff's contractors located abroad will also be produced to Defendants.

AMENDED RESPONSE TO INTERROGATORY NO. 6:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement or amend its response as discovery in this case continues, Plaintiff amends its response as follows:

(1) Wikimedia communications with its community members. Between April 23, 2017 and December 31, 2017, Wikimedia's U.S. servers received HTTP/S requests from, and transmitted HTTP/S responses to, users in at least 242 non-U.S. countries, territories and regions. This figure is an estimate that was derived using MaxMind geolocation data to determine the country associated with the client IP of each HTTPS request transmitted to Wikimedia's servers in the United States.

(2) Wikimedia's internal log communications. Every time Wikimedia receives an HTTP/S request from a person accessing a Wikimedia Project webpage, it creates a corresponding log entry. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted approximately over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between January 1, 2015 and December 12, 2017, Wikimedia's office network router located in the United States logged open Internet connections with at least approximately 221 non-U.S. countries, territories and regions.

This figure represents Internet outbound communications sent via the following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

This figure includes, but is not limited to, certain communications sent through

Wikimedia's Virtual Private Network (VPN).

This figure does not account for a significant number of Internet communications by Wikimedia staff and contractors located internationally who routinely communicate with Wikimedia staff and others located in the United States without using Wikimedia's Virtual Private Network. Between January 1, 2015 and December 22, 2017, Wikimedia engaged over 140 contractors, located across approximately 45 different countries.

The results of these analyses have been produced to Defendants. *See* WIKI0006146, WIKI0006147, WIKI0006148, WIKI0006149, WIKI0006282, WIKI0006368. An anonymized list of Plaintiff's contractors located abroad has also been produced to Defendants. *See* WIKI0006367.

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 6:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement its response as discovery in this case continues, Plaintiff supplements its response as follows:

The results of additional analyses on these three categories of communications are contained in response to Defendant Office of the Director of National Intelligence's Interrogatory No. 19.

INTERROGATORY NO. 7:

For each category of Wikimedia international, text-based, Internet communications identified in response to Interrogatory No. 3, above, that Plaintiff contends is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, please state the total number of such Wikimedia communications made to and from the United States each year for the years 2008-2017, specifying in each case the manner in which Wikimedia counts the communications

in that category (e.g., by site visit, page view, HTTP or HTTPS transmissions, e-mails, other forms of messaging, etc.).

RESPONSE TO INTERROGATORY NO. 7:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is vastly overbroad, unduly burdensome and seeks information that is not reasonably calculated to lead to the discovery of admissible evidence. Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, see ECF No. 116 at 4, and as ordered by the Court.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

(1) Wikimedia communications with its community members. Between April 23, 2017 and December 31, 2017, Wikimedia's U.S. servers received over 500 billion HTTPS requests from users outside of the United States. Each HTTPS request generates a corresponding response; thus Wikimedia exchanged over 1 trillion HTTPS requests and responses with its users between April 23, 2017 and December 31, 2017. These figures are estimates that were derived using MaxMind geolocation data to determine the country associated with the client IP of each HTTPS request transmitted to Wikimedia's servers in the United States.

(2) Wikimedia's internal log communications. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted approximately over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between June 4, 2014 and

December 12, 2017, Wikimedia's office network router located in the United States made at least approximately 22,934,372 Internet connections to 223 non-U.S. countries, territories and regions.

This figure is an estimate and was derived using a geolocation database that catalogues the IP addresses associated with each country, territory and region for each log entry obtained from the Wikimedia Foundation's office router.

This figure represents the total number of Internet outbound connections sent via the following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

This figure includes connections sent through Wikimedia's Virtual Private Network (VPN).

This figure does not account for the significant number of Internet communications by Wikimedia staff and contractors located internationally who did not communicate using Wikimedia's Virtual Private Network, but who routinely communicate with Wikimedia staff located at the U.S. headquarters. Between January 1, 2015 and December 22, 2017, Wikimedia engaged over 80 contractors, located across more than 30 different countries.

The results of these analyses will be produced to Defendants. An anonymized list of Plaintiff's contractors located abroad will also be produced to Defendants.

AMENDED RESPONSE TO INTERROGATORY NO. 7:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement or amend its response as discovery in this case continues, Plaintiff amends its response as follows:

(1) Wikimedia communications with its community members. Between April 23, 2017 and December 31, 2017, Wikimedia's U.S. servers received approximately over 511 billion

HTTP/S requests from users outside of the United States. Each HTTP/S request generates a corresponding response; thus Wikimedia exchanged over 1 trillion HTTP/S requests and responses with its users between April 23, 2017 and December 31, 2017.

These figures are estimates that were derived using MaxMind geolocation data to determine the country associated with the client IP of each HTTP/S request transmitted to Wikimedia's servers in the United States.

(2) Wikimedia's internal log communications. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted approximately over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between June 4, 2014 and December 12, 2017, Wikimedia's office network router located in the United States logged open Internet connections at least approximately 22,934,372 times, with 223 non-U.S. countries, territories and regions.

This figure is an estimate and was derived using a geolocation database that catalogues the IP addresses associated with each country, territory and region for each log entry obtained from the Wikimedia Foundation's office router.

This figure represents the total number of Internet outbound connections sent via the following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

This figure includes, but is not limited to, connections sent through Wikimedia's Virtual Private Network (VPN).

This figure does not account for a significant number of Internet communications by Wikimedia staff and contractors located internationally who routinely communicate with

Wikimedia staff and others located in the United States without using Wikimedia's Virtual Private Network. Between January 1, 2015 and December 22, 2017, Wikimedia engaged over 140 contractors, located across approximately 45 different countries.

The results of these analyses have been produced to Defendants. *See* WIKI0006146, WIKI0006147, WIKI0006148, WIKI0006149, WIKI0006282, WIKI0006368. An anonymized list of Plaintiff's contractors located abroad has also been produced to Defendants. *See* WIKI0006367.

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 7:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement its response as discovery in this case continues, Plaintiff supplements its response as follows:

The results of additional analyses on these three categories of communications are contained in response to Defendant Office of the Director of National Intelligence's Interrogatory No. 19.

INTERROGATORY NO. 8:

For each category of Wikimedia international, text-based, Internet communications identified in response to Interrogatory No. 3, above, that Plaintiff contends is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, please state by foreign country the number of such Wikimedia communications made to or from the United States each year for the years 2008-2017, specifying in each case the manner in which Wikimedia counts the communications in that category (e.g., by site visit, page view, HTTP or HTTPS transmissions, e-mails, other forms of messaging, etc.).

RESPONSE TO INTERROGATORY NO. 8:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is vastly overbroad, unduly burdensome and seeks information that is not reasonably calculated to lead to the discovery of admissible evidence. Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and as ordered by the Court. Plaintiff additionally objects to this Interrogatory as duplicative of other written discovery propounded by Defendants.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

(1) Wikimedia communications with its community members. The number of HTTPS requests that Wikimedia's U.S. servers received from users in each country, territory, or region between April 23, 2017 and December 31, 2017 is attached as Exhibit B and will be included in a forthcoming production to Defendants. Each HTTPS request generates a corresponding response that is not reflected in the figures included in this analysis. These figures are estimates that were derived using MaxMind geolocation data to determine the country associated with the client IP of each HTTPS request transmitted to Wikimedia's servers in the United States.

(2) Wikimedia's internal log communications. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between June 4, 2014 and

December 12, 2017, Wikimedia's office network router located in the United States sent at least approximately 22,934,372 Internet connections to at least 223 non-U.S. countries, territories and regions. A list of the numbers of these communications broken down by country, territory, or region will be produced to Defendants.

These figures are estimates and were derived using a geolocation database that catalogues the IP addresses associated with each country, territory and region for each log entry obtained from the Wikimedia Foundation's office router.

These figures represent the total number of Internet outbound connections sent via the following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

These figures include connections sent through Wikimedia's Virtual Private Network (VPN).

These figures do not account for the significant number of Internet communications by Wikimedia staff and contractors located internationally who did not communicate using Wikimedia's Virtual Private Network, but who routinely communicate with Wikimedia staff located at the U.S. headquarters. Between January 1, 2015 and December 22, 2017, Wikimedia engaged over 80 contractors, located across more than 30 different countries.

The results of these analyses will be produced to Defendants. An anonymized list of Plaintiff's staff and contractors located abroad will also be produced to Defendants.

AMENDED RESPONSE TO INTERROGATORY NO. 8:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement or amend its response as discovery in this case continues, Plaintiff amends its response as follows:

(1) Wikimedia communications with its community members. The number of HTTP/S requests that Wikimedia's U.S. servers received from users in each country, territory, or region between April 23, 2017 and December 31, 2017 is attached as Amended Exhibit B. Each HTTP/S request generates a corresponding response that is not reflected in the figures included in this analysis. These figures are estimates that were derived using MaxMind geolocation data to determine the country associated with the client IP of each HTTP/S request transmitted to Wikimedia's servers in the United States.

(2) Wikimedia's internal log communications. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted approximately over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between June 4, 2014 and December 12, 2017, Wikimedia's office network router located in the United States logged open Internet connections at least approximately 22,934,372 times with 223 non-U.S. countries, territories and regions. A list of the numbers of these communications broken down by country, territory, or region will be produced to Defendants.

This figure is an estimate and was derived using a geolocation database that catalogues the IP addresses associated with each country, territory and region for each log entry obtained from the Wikimedia Foundation's office router.

This figure represents the total number of Internet outbound connections sent via the following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

This figure includes, but is not limited to, connections sent through Wikimedia's Virtual Private Network (VPN).

This figure does not account for a significant number of Internet communications by Wikimedia staff and contractors located internationally who routinely communicate with Wikimedia staff and others located in the United States without using Wikimedia's Virtual Private Network. Between January 1, 2015 and December 22, 2017, Wikimedia engaged over 140 contractors, located across approximately 45 different countries.

The results of these analyses have been produced to Defendants. *See* WIKI0006146, WIKI0006147, WIKI0006148, WIKI0006149, WIKI0006282, WIKI0006368. An anonymized list of Plaintiff's staff and contractors located abroad has also been produced to Defendants. *See* WIKI0006367.

SECOND AMENDED RESPONSE TO INTERROGATORY NO. 8:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement or amend its response as discovery in this case continues, Plaintiff amends its response as follows:

(1) Wikimedia communications with its community members. The number of HTTP/S requests that Wikimedia's U.S. servers received from users in each country, territory, or region between April 23, 2017 and December 31, 2017 is attached as Amended Exhibit B. The number of HTTP requests that Wikimedia's U.S. servers received from users in each country, territory, or region between August 1, 2017 and January 31, 2018 is attached as Supplemental Exhibit C. The number of HTTPS requests that Wikimedia's U.S. servers received from users in each country territory, or region between August 1, 2017 and January 31, 2018 is attached as Supplemental Exhibit D. Each HTTP/S request generates a corresponding response that is not reflected in the figures included in this analysis. These figures are estimates that were derived using MaxMind geolocation data to determine the country associated with the client IP of each

HTTP/S request transmitted to Wikimedia's servers in the United States.

(2) Wikimedia's internal log communications. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted approximately over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between June 4, 2014 and December 12, 2017, Wikimedia's office network router located in the United States logged open Internet connections at least approximately 22,934,372 times with 223 non-U.S. countries, territories and regions. A list of the numbers of these communications broken down by country, territory, or region will be produced to Defendants.

This figure is an estimate and was derived using a geolocation database that catalogues the IP addresses associated with each country, territory and region for each log entry obtained from the Wikimedia Foundation's office router.

This figure represents the total number of Internet outbound connections sent via the following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

This figure includes, but is not limited to, connections sent through Wikimedia's Virtual Private Network (VPN).

This figure does not account for a significant number of Internet communications by Wikimedia staff and contractors located internationally who routinely communicate with Wikimedia staff and others located in the United States without using Wikimedia's Virtual Private Network. Between January 1, 2015 and December 22, 2017, Wikimedia engaged over 140 contractors, located across approximately 45 different countries.

The results of these analyses have been produced to Defendants. *See* WIKI0006146,

WIKI0006147, WIKI0006148, WIKI0006149, WIKI0006282, WIKI0006368. An anonymized list of Plaintiff's staff and contractors located abroad has also been produced to Defendants. *See* WIKI0006367.

The results of additional analyses on these three categories of communications are contained in response to Defendant Office of the Director of National Intelligence's Interrogatory No. 19.

INTERROGATORY NO. 11:

Please state the basis of Plaintiff's allegations, in paragraphs 61, 85, and 88 of the Amended Complaint, that Wikimedia's alleged "community of volunteers, contributors, and readers consists of individuals in virtually every country on earth" and that Wikimedia "communicate[s] with individuals in virtually every country on earth."

RESPONSE TO INTERROGATORY NO. 11:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is overbroad and duplicative of other written discovery propounded by Defendants. Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

Numerous facts support Wikimedia's allegations that its "community of volunteers, contributors, and readers consists of individuals in virtually every country on earth" and that Wikimedia engages in "communications . . . with individuals in virtually every country on earth." As explained in Wikimedia's responses to NSA Interrogatory Nos. 6-8, Wikimedia users from all over the world read and contribute to Wikimedia's Project pages. This analysis is further supported by statistics showing that Wikimedia's Project pages are viewed by millions of users around the world. Wikimedia publishes current monthly page view statistics by country

(*available* at https://stats.wikimedia.org/wikimedia/squids/SquidReportPageViewsPerCountryOverview.htm), and maintains an archive with analogous data for past months (*available* at https://stats.wikimedia.org/archive/squid_reports/).

Wikimedia also has dozens of foreign independent but associated entities, including user groups, chapters and thematic organizations. *See* https://meta.wikimedia.org/wiki/Wikimedia_movement_affiliates#chapters.

In the last two years alone, Wikimedia has awarded grants and scholarships to users and programs in dozens of countries. Additionally, Wikimedia projects are currently active in 288 languages, further underscoring Wikimedia's global presence. *See* https://en.wikipedia.org/wiki/List_of_Wikipedias.

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 11:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement its response as discovery in this case continues, Plaintiff supplements its response as follows:

Wikimedia also maintains a publicly available repository of data that allows for various analyses of Wikimedia project page views by country (*available* at https://wikitech.wikimedia.org/wiki/Analytics/AQS/Pageviews).

Numerous documents in Plaintiff's production support its allegations that its "community of volunteers, contributors, and readers consists of individuals in virtually every country on earth" and that Wikimedia engages in "communications . . . with individuals in virtually every country on earth," including, *inter alia*, Amended Exhibit B; WIKI0006367 (listing international Wikimedia contractors); WIKI0002407 (listing 288 Wikipedia language editions);

WIKI0002416 (listing Wikimedia movement affiliates); WIKI0006369 (listing page views for virtually every country on earth); WIKI0002360, WIKI0002365, WIKI0002367, WIKI0002389, WIKI0002396 (noting countries involved in user grants and scholarships); WIKI0006295 (listing funded grants by country).

SECOND SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 11:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement its response as discovery in this case continues, Plaintiff supplements its response as follows:

Numerous other statistics produced by Plaintiff show that Wikimedia's community of volunteers, contributors, and readers consists of individuals in virtually every country on earth, and that Wikimedia engages in communications with individuals in virtually every country on earth. *See* WIKI0009301, WIKI0008312, WIKI0008313, WIKI0007616, WIKI0009269, WIKI0008265, WIKI0008271, WIKI0008262, WIKI0009224, WIKI0009234.

ALLEGATIONS REGARDING NSA INTERCEPTION OF WIKIMEDIA'S INTERNATIONAL, TEXT-BASED, INTERNET COMMUNICATIONS

INTERROGATORY NO. 14:

Please state the basis of Plaintiff's allegation, in paragraph 49 of the Amended Complaint, that Upstream surveillance includes a process in which the NSA makes a copy of international text-based communications flowing across certain high-capacity cables, switches, and routers along the Internet backbone.

RESPONSE TO INTERROGATORY NO. 14:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is duplicative of other written discovery propounded by Defendants.

Plaintiff additionally objects that these matters may be the subject of expert reports and

testimony, as to which Plaintiff will provide discovery at the appropriate time.

Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

The bases of Plaintiff's allegation are the principles of Internet communication and the technical necessities of the inspection of Internet communications in transit.

For example, Internet communications in transit are split into packets. Where an eavesdropper is attempting to determine whether the contents of a particular communication in transit on the Internet contain a particular piece of information, the eavesdropper generally must reassemble the packets constituting the communication and then scan the reassembled communication. Reassembling Internet packets requires the temporary copying (or "caching") of those packets until all packets needed for the reassembly have arrived.

Additionally, Upstream surveillance involves the retention of communications that contain targeted selectors. To retain a communication in transit, an eavesdropper must copy and reassemble the packets constituting the communication. But because an eavesdropper cannot know in advance which packets in transit are part of a communication containing a targeted selector, the eavesdropper must create a temporary copy of all packets that might be a part of such a communication.

In addition, a *New York Times* report from August 2013 states, based on a review of NSA documents and interviews with senior intelligence officials, that "the N.S.A. is temporarily copying and then sifting through the contents of what is apparently most e-mails and other textbased communications that cross the border." Charlie Savage, *N.S.A Said to Search Content*

of Messages to and from U.S., N.Y. Times, Aug. 8, 2013; *see also* Charlie Savage, *Power Wars* 207–11 (2015).

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 14:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement its response as discovery in this case continues, Plaintiff supplements its response as follows:

The bases for Plaintiff's allegation also include the following:

- Executive Office of the President of the United States, The Comprehensive National Cybersecurity Initiative
- U.S. Dep't of Homeland Security, Privacy Impact Assessment for the Initiative Three Exercise (Mar. 18, 2010)
- OLC, Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (Einstein 2.0) to Protect Unclassified Computer Networks in the Executive Branch (Jan. 9, 2009)
- U.S. Dep't of Homeland Security, Privacy Impact Assessment for Einstein 3 – Accelerated (E3A) (Apr. 19, 2013)
- U.S. Dep't of Homeland Security, Privacy Impact Assessment for Einstein 2 (May 19, 2008)

INTERROGATORY NO. 15:

Please state the basis of Plaintiff's contentions regarding the manner in which the alleged copying, filtering, and content-review processes referred to in paragraph 49 of the Amended Complaint are carried out.

RESPONSE TO INTERROGATORY NO. 15:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is a contention Interrogatory that is premature at this stage in the litigation. Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time.

Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery. Plaintiff also objects that this Interrogatory is overbroad and duplicative of other written discovery propounded by Defendants.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

The bases of Plaintiff's contentions are the principles of Internet communication and the technical necessities of the inspection of Internet communications in transit.

For example, Internet communications in transit are split into packets. Where an eavesdropper is attempting to determine whether the contents of a particular communication in transit on the Internet contain a particular piece of information, the eavesdropper generally must reassemble the packets constituting the communication and then scan the reassembled communication. Reassembling Internet packets requires the temporary copying (or "caching") of those packets until all packets needed for the reassembly have arrived.

Additionally, Upstream surveillance involves the retention of communications that contain targeted selectors. To retain a communication in transit, an eavesdropper must copy and reassemble the packets constituting the communication. But because an eavesdropper cannot know in advance which packets in transit are part of a communication containing a targeted selector, the eavesdropper must create a temporary copy of all packets that might be a part of

such a communication.

In addition, a *New York Times* report from August 2013 states, based on a review of NSA documents and interviews with senior intelligence officials, that "the N.S.A. is temporarily copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border." Charlie Savage, *N.S.A Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013; *see also* Charlie Savage, *Power Wars* 207–11 (2015).

Other bases of Plaintiff's contentions include:

- The PCLOB Report, including pages 7–10, 12–13, 22, 30–41 & n.157, 79, 111 n.476, 120–22, 125, 143, and official government sources concerning Upstream surveillance cited therein.
- [*Redacted*], No. [Redacted], 2011 WL 10945618 (FISC Oct. 3, 2011)
- 50 U.S.C. §§ 1801, 1881a.
- David S. Kris & J. Douglas Wilson, *National Security Investigations and Prosecutions* § 17.5 (July 2015)
- Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents)
- Julia Angwin & Jeff Larson, *New Snowden Documents Reveal Secret Memos Expanding Spying*, ProPublica, June 4, 2015 (and associated documents)
- Jeff Larson et al., *A Trail of Evidence Leading to AT&T's Partnership with the NSA*, ProPublica, Aug. 15, 2015 (and associated documents)
- PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 26:15–18 (Mar. 19, 2014) (statement of

Robert Litt, General Counsel, ODNI)

- Charlie Savage, *Power Wars* (2015)

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 15:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement as discovery in this case continues, Plaintiff supplements its response as follows:

The bases for Plaintiff's contention also include the following: Glenn Greenwald, *No Place to Hide* (2014).

SECOND SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 15:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement as discovery in this case continues, Plaintiff supplements its response as follows:

The bases for Plaintiff's contentions also include the following:

- PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (Mar. 19, 2014)
- PCLOB, Public Hearing Regarding Consideration of Recommendations for Change: The Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act (Nov. 4, 2013)
- June 1, 2011 FISC submission
- July 15, 2015 FISC submission (2015 Summary of Notable Section 702 Requirements)
- June 28, 2011 FISC submission
- August 16, 2011 FISC submission

- November 15, 2011 FISC submission (Government's Responses to FISC Questions Re: Amended 2011 Section 702 Certifications)
- FISC Opinion (Sept. 25, 2012)
- FISC Opinion (Apr. 26, 2017)
- NSA Section 702 Targeting Procedures
- NSA Section 702 Minimization Procedures
- PCLOB, Recommendations Assessment Reports
- ODNI, Statistical Transparency Reports Regarding the Use of National Security Authorities
- Executive Office of the President of the United States, The Comprehensive National Cybersecurity Initiative
- U.S. Dep't of Homeland Security, Privacy Impact Assessment for the Initiative Three Exercise (Mar. 18, 2010)
- OLC, Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (Einstein 2.0) to Protect Unclassified Computer Networks in the Executive Branch (Jan. 9, 2009)
- U.S. Dep't of Homeland Security, Privacy Impact Assessment for Einstein 3 – Accelerated (E3A) (Apr. 19, 2013)
- U.S. Dep't of Homeland Security, Privacy Impact Assessment for Einstein 2 (May 19, 2008)
- ODNI, Conference Call with the Press Addressing Multi-Communication Transactions (Aug. 21, 2013)

INTERROGATORY NO. 17:

Please state the basis of Plaintiff's allegations, in paragraphs 62 and 64 of the Amended Complaint, respectively, that "in order for the NSA to reliably obtain communications to, from, or about its targets in the way it has described, the government must be copying and reviewing all the international text-based communications that travel across a given link," and that "for every backbone link that the NSA monitors using Upstream surveillance, the monitoring must be comprehensive in order for the government to accomplish its stated goals."

RESPONSE TO INTERROGATORY NO. 17:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff also objects that this Interrogatory is duplicative of other written discovery propounded by Defendants. Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time. Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

Plaintiff's allegation is based on basic principles governing the routing and transmission of Internet communications, as well as basic principles governing how surveillance on a packet-switched network operates.

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 17:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement as discovery in this case continues, Plaintiff supplements its

response as follows:

The bases for Plaintiff's allegations also include the following:

- PCLOB Report and official government sources concerning Upstream surveillance cited therein.
- [*Redacted*], No. [Redacted], 2011 WL 10945618 (FISC Oct. 3, 2011)
- 50 U.S.C. §§ 1801, 1881a
- David S. Kris & J. Douglas Wilson, *National Security Investigations and Prosecutions* § 17.5 (July 2015)
- Julia Angwin & Jeff Larson, *New Snowden Documents Reveal Secret Memos Expanding Spying*, ProPublica (June 4, 2015) (and associated documents)
- Julia Angwin et al., *AT&T Helped U.S. Spy on Internet on Vast Scale*, N.Y. Times, Aug. 15, 2015 (and associated documents)
- Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents)
- Jeff Larson et al., *A Trail of Evidence Leading to AT&T's Partnership with the NSA*, ProPublica, Aug. 15, 2015 (and associated documents)
- Charlie Savage, *Power Wars* (2015)
- Charlie Savage, *N.S.A. Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013
- Glenn Greenwald, *No Place to Hide* (2014)
- PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (Mar. 19, 2014)

- PCLOB, Public Hearing Regarding Consideration of Recommendations for Change: The Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act (Nov. 4, 2013)
- June 1, 2011 FISC submission
- July 15, 2015 FISC submission (2015 Summary of Notable Section 702 Requirements)
- June 28, 2011 FISC submission
- August 16, 2011 FISC submission
- November 15, 2011 FISC submission (Government's Responses to FISC Questions Re: Amended 2011 Section 702 Certifications)
- FISC Opinion (Sept. 25, 2012)
- FISC Opinion (Apr. 26, 2017)
- NSA Section 702 Targeting Procedures
- NSA Section 702 Minimization Procedures
- PCLOB, Recommendations Assessment Reports
- ODNI, Statistical Transparency Reports Regarding the Use of National Security Authorities
- Executive Office of the President of the United States, The Comprehensive National Cybersecurity Initiative
- U.S. Dep't of Homeland Security, Privacy Impact Assessment for the Initiative Three Exercise (Mar. 18, 2010)

- OLC, Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (Einstein 2.0) to Protect Unclassified Computer Networks in the Executive Branch (Jan. 9, 2009)
- U.S. Dep't of Homeland Security, Privacy Impact Assessment for Einstein 3 – Accelerated (E3A) (Apr. 19, 2013)
- U.S. Dep't of Homeland Security, Privacy Impact Assessment for Einstein 2 (May 19, 2008)

INTERROGATORY NO. 20:

Please state the basis of Plaintiff's allegations, in paragraphs 65 and 66 of the Amended Complaint, that in conducting Upstream surveillance "the government's aim is to 'comprehensively' … obtain communications to, from, and about targets scattered around the world," and that "the government is interested in obtaining, with a high degree of confidence, all international communications to, from, or about its targets."

RESPONSE TO INTERROGATORY NO. 20:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is duplicative of other written discovery propounded by Defendants. Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

The PCLOB has described the use of Upstream surveillance to collect "about" communications as "an inevitable byproduct of the government's efforts to comprehensively acquire communications that are sent to or from its targets." PCLOB Report 10. And it has said

about Upstream surveillance more generally that this method's "success . . . depends on collection devices that can *reliably* acquire data packets associated with the proper communications." *Id.* at 143 (emphasis added); *see also* PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 26:15–18 (Mar. 19, 2014) (statement of Robert Litt, General Counsel, ODNI).

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 20:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement as discovery in this case continues, Plaintiff supplements its response as follows:

The bases for Plaintiff's allegations also include the following:

- [*Redacted*], No. [Redacted], 2011 WL 10945618 (FISC Oct. 3, 2011)
- PCLOB Report and official government sources concerning Upstream surveillance cited therein
- PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (Mar. 19, 2014)
- PCLOB, Public Hearing Regarding Consideration of Recommendations for Change: The Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act (Nov. 4, 2013)
- The document attached as Exhibit A to Plaintiff's First Set of Requests for Admission, "Why are we interested in HTTP?"
- Glenn Greenwald, *Xkeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet'*, The Guardian, July 31, 2013 (and associated documents).

- Julia Angwin & Jeff Larson, *New Snowden Documents Reveal Secret Memos Expanding Spying*, ProPublica (June 4, 2015) (and associated documents)
- Julia Angwin et al., *AT&T Helped U.S. Spy on Internet on Vast Scale*, N.Y. Times, Aug. 15, 2015 (and associated documents)
- Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents)
- Jeff Larson et al., *A Trail of Evidence Leading to AT&T's Partnership with the NSA*, ProPublica, Aug. 15, 2015 (and associated documents)
- Charlie Savage, *Power Wars* (2015)
- Charlie Savage, *N.S.A. Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013
- Glenn Greenwald, *No Place to Hide* (2014)

Dated: April 17, 2018

/s/Ashley Gorski

Ashley Gorski
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
agorski@aclu.org

Counsel for Plaintiff Wikimedia Foundation, Inc.

SUPPLEMENTAL EXHIBIT C

Foreign Country, Territory, or Region	Number of HTTP Requests to Wikimedia's Servers in the United States from August 1, 2017 to January 31, 2018
Afghanistan	821,201
Åland	378
Albania	51,889
Algeria	843,262
Andorra	2,992
Angola	725,015
Anguilla	64,496
Antigua and Barbuda	725,010
Argentina	144,245,201
Armenia	167,659
Aruba	1,313,447
Australia	280,363,407
Austria	1,370,265
Azerbaijan	889,617
Bahamas	2,846,518
Bahrain	53,444
Bangladesh	26,717,162
Barbados	2,921,683
Belarus	489,593
Belgium	2,627,346
Belize	1,081,373

Benin	159,654
Bermuda	1,003,422
Bhutan	718,888
Bolivia	16,027,273
Bonaire, Sint Eustatius, and Saba	288,802
Bosnia and Herzegovina	36,230
Botswana	15,182
Brazil	743,523,019
British Indian Ocean Territory	143
British Virgin Islands	269,290
Brunei	1,434,086
Bulgaria	158,583
Burkina Faso	476,477
Burundi	186,611
Cabo Verde	5,301
Cambodia	9,423,280
Cameroon	828,395
Canada	626,430,503
Cayman Islands	1,266,819
Central African Republic	6,531
Chad	199,040
Chile	74,786,914
China	1,887,127,378

Christmas Island	8,375
Cocos [Keeling] Islands	923
Colombia	121,075,673
Comoros	3,666
Congo	1,074,674
Cook Islands	46,884
Costa Rica	22,372,501
Croatia	96,896
Cuba	719,445
Curaçao	2,678,493
Cyprus	124,788
Czechia	722,782
Denmark	215,876
Djibouti	20,527
Dominica	103,744
Dominican Republic	30,822,853
East Timor	181,512
Ecuador	55,544,542
Egypt	331,832
El Salvador	9,873,835
Equatorial Guinea	4,439
Eritrea	523
Estonia	66,476

Ethiopia	644,743
Falkland Islands	189
Faroe Islands	841
Federated States of Micronesia	64,610
Fiji	954,395
Finland	4,776,759
France	5,203,094
French Guiana	369,332
French Polynesia	895,747
French Southern Territories	7
Gabon	111,299
Gambia	38,860
Georgia	152,626
Germany	29,673,372
Ghana	290,814
Gibraltar	1,286
Greece	146,110
Greenland	600,633
Grenada	714,389
Guadeloupe	1,078,725
Guatemala	14,782,703
Guernsey	1,147
Guinea	329,981

Guinea-Bissau	19,274
Guyana	1,995,531
Haiti	1,799,389
Hashemite Kingdom of Jordan	748,358
Honduras	10,918,870
Hong Kong	132,445,801
Hungary	240,405
Iceland	26,267
India	262,028,913
Indonesia	454,933,133
Iran	33,154,224
Iraq	736,244
Ireland	593,762,872
Isle of Man	1,492
Israel	1,702,244
Italy	5,751,959
Ivory Coast	26,827
Jamaica	6,257,705
Japan	626,903,248
Jersey	5,088
Kazakhstan	233,815
Kenya	325,857
Kiribati	11,431

Kosovo	2,063
Kuwait	115,962
Kyrgyzstan	129,540
Laos	2,771,786
Latvia	67,497
Lebanon	226,570
Lesotho	91,060
Liberia	170,511
Libya	93,489
Liechtenstein	1,340
Luxembourg	40,681
Macao	4,414,341
Macedonia	30,060
Madagascar	211,134
Malawi	53,964
Malaysia	85,171,046
Maldives	2,314,246
Mali	169,424
Malta	47,636
Marshall Islands	38,106
Martinique	2,889,796
Mauritania	43,870
Mauritius	51,118

Mayotte	1,032
Mexico	276,945,398
Monaco	3,871
Mongolia	3,098,609
Montenegro	36,032
Montserrat	28,283
Morocco	495,003
Mozambique	110,182
Myanmar [Burma]	3,574,699
Namibia	15,794
Nauru	9,882
Nepal	14,121,673
Netherlands	38,092,032
New Caledonia	841,889
New Zealand	52,447,130
Nicaragua	8,800,538
Niger	59,676
Nigeria	523,467
Niue	4,402
Norfolk Island	4,200
North Korea	4,524
Norway	1,177,129
Oman	66,102

Pakistan	10,812,865
Palau	50,597
Palestine	157,595
Panama	19,029,566
Papua New Guinea	335,250
Paraguay	9,064,249
Peru	24,219,191
Philippines	89,704,175
Pitcairn Islands	36
Poland	2,958,397
Portugal	147,617
Qatar	156,184
Republic of Korea	690,307,638
Republic of Lithuania	69,788
Republic of Moldova	101,328
Republic of the Congo	52,530
Romania	393,888
Russia	2,680,016
Rwanda	414,825
Réunion	43,662
Saint Helena	38
Saint Kitts and Nevis	26,495
Saint Lucia	645,483

Saint Martin	101,279
Saint Pierre and Miquelon	29,128
Saint Vincent and the Grenadines	501,327
Saint-Barthélemy	3,287
Samoa	32,278
San Marino	272
Saudi Arabia	422,297
Senegal	122,076
Serbia	146,019
Seychelles	6,810
Sierra Leone	173,742
Singapore	189,603,688
Sint Maarten	375,159
Slovak Republic	4,858
Slovakia	95,273
Slovenia	26,343
Solomon Islands	40,868
Somalia	93,633
South Africa	473,077
South Georgia and the South Sandwich Islands	123
South Sudan	220,658
Spain	1,035,451
Sri Lanka	510,052

St Kitts and Nevis	324,512
Sudan	193,786
Suriname	1,613,129
Svalbard and Jan Mayen	73
Swaziland	110,645
Sweden	774,442
Switzerland	1,647,426
Syria	282,939
São Tomé and Príncipe	1,157
Taiwan	119,710,225
Tajikistan	334,945
Tanzania	617,298
Thailand	114,379,182
Togo	71,240
Tokelau	403
Tonga	30,399
Trinidad and Tobago	8,100,970
Tunisia	200,575
Turkey	28,568,637
Turkmenistan	38,007
Turks and Caicos Islands	564,567
Tuvalu	1,542
Uganda	1,741,953

Ukraine	2,377,191
United Arab Emirates	762,824
United Kingdom	15,128,140
Uruguay	9,577,567
Uzbekistan	268,916
Vanuatu	72,277
Vatican City	77
Venezuela	64,068,797
Vietnam	417,965,885
Wallis and Futuna	12,486
Western Sahara	10
Yemen	139,189
Zambia	714,196
Zimbabwe	961,529

SUPPLEMENTAL EXHIBIT D

Foreign Country, Territory, or Region	Number of HTTPS Requests to Wikimedia's Servers in the United States from August 1, 2017 to January 31, 2018
Afghanistan	20,604,532
Åland	133,943
Albania	9,643,581
Algeria	128,780,026
Andorra	265,822
Angola	113,578,445
Anguilla	2,217,119
Antigua and Barbuda	34,519,166
Argentina	13,052,041,069
Armenia	16,619,809
Aruba	46,034,224
Australia	19,425,507,629
Austria	43,074,736
Azerbaijan	92,885,398
Bahamas	112,093,153
Bahrain	6,954,957
Bangladesh	2,385,092,865
Barbados	115,182,398
Belarus	81,967,203
Belgium	60,091,900
Belize	51,618,265
Benin	23,946,277
Bermuda	40,147,959
Bhutan	36,331,354

Bolivia	1,404,857,896
Bonaire, Sint Eustatius, and Saba	10,085,028
Bosnia and Herzegovina	7,020,177
Botswana	2,451,091
Brazil	31,015,286,204
British Indian Ocean Territory	12,169
British Virgin Islands	4,623,366
Brunei	156,296,973
Bulgaria	30,331,597
Burkina Faso	82,427,481
Burundi	30,241,949
Cabo Verde	920,646
Cambodia	369,780,518
Cameroon	133,484,746
Canada	36,379,477,322
Cayman Islands	39,135,595
Central African Republic	1,415,519
Chad	34,068,856
Chile	6,726,153,714
China	7,835,059,394
Christmas Island	352,364
Cocos [Keeling] Islands	115,575
Colombia	11,515,675,774
Comoros	1,317,537
Congo	228,406,703
Cook Islands	2,939,189

Costa Rica	1,262,430,752
Croatia	16,927,085
Cuba	186,179,730
Curaçao	59,625,943
Cyprus	6,689,187
Czechia	58,231,479
Denmark	38,271,882
Djibouti	2,140,379
Dominica	8,080,763
Dominican Republic	2,151,854,032
East Timor	24,375,421
Ecuador	3,860,446,842
Egypt	57,100,043
El Salvador	882,209,181
Equatorial Guinea	680,068
Eritrea	60,304
Estonia	8,603,956
Ethiopia	84,571,842
Falkland Islands	18,642
Faroe Islands	158,452
Federated States of Micronesia	4,517,004
Fiji	77,928,890
Finland	29,158,348
France	358,230,836
French Guiana	19,324,082
French Polynesia	80,847,556

French Southern Territories	736
Gabon	27,078,961
Gambia	6,384,517
Georgia	22,408,026
Germany	562,211,287
Ghana	46,368,618
Gibraltar	306,873
Greece	46,363,715
Greenland	14,325,826
Grenada	27,344,536
Guadeloupe	66,885,212
Guatemala	1,472,820,804
Guernsey	334,080
Guinea	83,260,527
Guinea-Bissau	4,255,517
Guyana	79,823,616
Haiti	265,132,981
Hashemite Kingdom of Jordan	91,259,008
Honduras	744,069,894
Hong Kong	8,716,103,273
Hungary	47,081,457
Iceland	2,711,278
India	3,165,955,918
Indonesia	13,116,466,025
Iran	87,510,049
Iraq	24,405,997

Ireland	2,112,117,966
Isle of Man	341,100
Israel	62,141,461
Italy	210,385,545
Ivory Coast	3,970,928
Jamaica	395,757,541
Japan	85,441,052,143
Jersey	345,920
Kazakhstan	44,137,526
Kenya	49,280,668
Kiribati	1,689,164
Kosovo	342,323
Kuwait	14,247,593
Kyrgyzstan	31,333,488
Laos	109,472,472
Latvia	9,104,225
Lebanon	13,599,863
Lesotho	13,499,426
Liberia	26,031,402
Libya	9,195,709
Liechtenstein	215,673
Luxembourg	5,639,047
Macao	411,561,258
Macedonia	5,123,868
Madagascar	58,417,988
Malawi	7,613,927

Malaysia	6,437,106,376
Maldives	94,625,241
Mali	37,296,988
Malta	2,509,967
Marshall Islands	2,897,907
Martinique	83,396,604
Mauritania	7,882,681
Mauritius	2,468,551
Mayotte	193,971
Mexico	26,039,248,714
Monaco	541,934
Mongolia	301,320,409
Montenegro	2,819,788
Montserrat	1,252,999
Morocco	76,616,817
Mozambique	22,792,076
Myanmar [Burma]	384,217,247
Namibia	1,070,964
Nauru	538,677
Nepal	598,746,931
Netherlands	204,649,528
New Caledonia	102,524,542
New Zealand	3,539,655,892
Nicaragua	456,108,803
Niger	12,480,647
Nigeria	50,500,001

Niue	225,126
Norfolk Island	235,514
North Korea	887,377
Norway	40,036,961
Oman	6,073,423
Pakistan	318,156,164
Palau	2,828,940
Palestine	11,032,480
Panama	1,189,381,456
Papua New Guinea	48,345,831
Paraguay	752,603,128
Peru	7,030,573,552
Philippines	9,277,043,820
Pitcairn Islands	23,977
Poland	228,061,723
Portugal	26,235,675
Qatar	14,554,687
Republic of Korea	8,320,136,352
Republic of Lithuania	11,873,194
Republic of Moldova	12,242,253
Republic of the Congo	12,001,830
Romania	100,552,982
Russia	288,064,755
Rwanda	41,922,847
Réunion	2,043,341
Saint Helena	16,961

Saint Kitts and Nevis	1,583,317
Saint Lucia	37,677,429
Saint Martin	4,577,110
Saint Pierre and Miquelon	5,106,171
Saint Vincent and the Grenadines	20,676,869
Saint-Barthélemy	317,643
Samoa	3,592,302
San Marino	42,125
Saudi Arabia	39,968,209
Senegal	22,533,953
Serbia	47,477,541
Seychelles	620,663
Sierra Leone	26,258,425
Singapore	5,131,135,255
Sint Maarten	11,305,651
Slovak Republic	1,121,120
Slovakia	16,705,364
Slovenia	5,575,086
Solomon Islands	8,907,274
Somalia	15,262,543
South Africa	34,949,275
South Georgia and the South Sandwich Islands	33,982
South Sudan	15,109,935
Spain	149,596,780
Sri Lanka	68,750,415
St Kitts and Nevis	13,753,545

Sudan	22,173,374
Suriname	78,396,254
Svalbard and Jan Mayen	1,408
Swaziland	15,120,981
Sweden	53,487,983
Switzerland	63,031,700
Syria	36,608,575
São Tomé and Príncipe	364,059
Taiwan	17,479,596,696
Tajikistan	67,222,492
Tanzania	58,174,269
Thailand	7,935,948,956
Togo	15,386,691
Tokelau	33,274
Tonga	3,723,043
Trinidad and Tobago	338,216,935
Tunisia	34,125,021
Turkey	1,118,611,571
Turkmenistan	1,258,697
Turks and Caicos Islands	8,998,062
Tuvalu	153,174
Uganda	190,307,650
Ukraine	520,208,217
United Arab Emirates	58,227,626
United Kingdom	574,948,730
Uruguay	1,374,562,931

Uzbekistan	32,395,981
Vanuatu	9,045,979
Vatican City	15,768
Venezuela	5,382,496,004
Vietnam	6,578,718,936
Wallis and Futuna	1,360,077
Western Sahara	3,664
Yemen	7,653,920
Zambia	94,948,340
Zimbabwe	61,649,107

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix BB

IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, INC. Plaintiff, v. NATIONAL SECURITY AGENCY, et al., Defendants.	Civil Action No. 1:15-cv-00662-TSE Hon. T.S. Ellis, III

WIKIMEDIA FOUNDATION, INC.'S AMENDED RESPONSES AND OBJECTIONS TO OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE'S INTERROGATORY NO. 19

PROPOUNDING PARTY: **OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**

RESPONDING PARTY: **WIKIMEDIA FOUNDATION, INC.**

SET NUMBER: **THREE**

Pursuant to Federal Rule of Civil Procedure 33, Plaintiff Wikimedia Foundation, Inc. ("Plaintiff" or "Wikimedia") responds as follows to Defendant Office of the Director of National Intelligence's ("Defendant" or "ODNI") (collectively with Plaintiff, the "Parties") Interrogatory No. 19 (the "Interrogatory"):

I. GENERAL RESPONSES.

1. Plaintiff's response to Defendant's Interrogatory is made to the best of Plaintiff's present knowledge, information, and belief. Discovery in this action is ongoing, and Plaintiff's responses may be substantially altered by further investigation, including further review of Plaintiff's own documents, as well as the review of documents produced by Defendant. Said response is at all times subject to such additional or different information that discovery or further investigation may disclose and, while based on the present state of Plaintiff's recollection, is

subject to such refreshing of recollection, and such additional knowledge of facts, as may result from Plaintiff's further discovery or investigation.

2. Plaintiff reserves the right to make any use of, or to introduce at any hearing and at trial, information and/or documents responsive to Defendant's Interrogatory but discovered subsequent to the date of this response, including, but not limited to, any such information or documents obtained in discovery herein.

3. To the extent that Plaintiff responds to Defendant's Interrogatory by stating that Plaintiff will provide information and/or documents that Plaintiff deems to embody material that is private, business confidential, proprietary, trade secret, or otherwise protected from disclosure pursuant to Federal Rule of Civil Procedure 26(c)(7), Federal Rule of Evidence 501, or other applicable law, Plaintiff will do so only pursuant to the Parties' Stipulated Protective Order (ECF No. 120).

4. Plaintiff reserves all objections or other questions as to the competency, relevance, materiality, privilege, or admissibility as evidence in any subsequent proceeding in or trial of this or any other action for any purpose whatsoever of Plaintiff's responses herein and any document or thing identified or provided in response to Defendant's Interrogatory.

5. Plaintiff's responses will be subject to and limited by any agreements the Parties reach concerning the scope of discovery.

6. Plaintiff reserves the right to object on any ground at any time to such other or supplemental interrogatories as Defendant may at any time propound involving or relating to the subject matter of this Interrogatory.

II. GENERAL OBJECTIONS.

Plaintiff makes the following general objections, whether or not separately set forth in

response to the Interrogatory, to each instruction, definition, and Interrogatory made in Defendant ODNI's Interrogatories, Set Three:

1. Plaintiff objects to the Interrogatory in its entirety insofar as the instructions, definitions, or Interrogatory seeks information or production of documents protected by the attorney-client privilege or the work product doctrine. Fed. R. Civ. Proc. 26(b)(1). Such information or documents shall not be provided in response to Defendant's Interrogatory and any inadvertent disclosure or production thereof shall not be deemed a waiver of any privilege with respect to such information or documents or of any work product immunity which may attach thereto. Fed. R. Civ. Proc. 26(b)(5)(B).

2. Plaintiff objects to the Interrogatory in its entirety to the extent the instruction, definition, or Interrogatory seeks identification of documents, witnesses, or information that Defendant has withheld from Plaintiff. Fed. R. Civ. Proc. 26(b)(1), (2).

3. Plaintiff objects to the Interrogatory in its entirety to the extent it requires Plaintiff to identify potentially thousands of pages of documents, not all of which have been or can be located and reviewed by counsel within the time period allowed for this response or within a reasonable time. Accordingly, the Interrogatory would subject Plaintiff to unreasonable and undue annoyance, oppression, burden and expense.

4. Plaintiff objects to the extent the Interrogatory exceeds the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and ordered by the Court. *See* ECF No. 117.

5. Plaintiff objects to the Interrogatory in its entirety to the extent it seeks information that is available through or from public sources or records, or that is otherwise equally available to Defendant, on the ground that it unreasonably subjects Plaintiff to undue annoyance, oppression,

burden, and expense. Fed. R. Civ. Proc. 26(b)(1), (2).

6. Plaintiff objects to the Interrogatory in its entirety to the extent it purports to impose obligations that are greater or more burdensome than or contradict those imposed by the applicable Federal and local rules. *See* Fed. R. Civ. Proc. 26, 33.

7. Plaintiff objects to the Interrogatory in its entirety as Defendant's Interrogatories in aggregate contain more than the "25 written interrogatories, including all discrete subparts," permitted by the Federal Rules of Civil Procedure, Rule 33(a)(1), and Defendant has not sought leave to serve additional interrogatories.

8. Plaintiff objects to the Interrogatory in its entirety to the extent it seeks documents or information no longer in existence or not currently in Plaintiff's possession, custody, or control, or to the extent it refers to persons, entities, or events not known to Plaintiff or controlled by Plaintiff, on the grounds that such definitions or Interrogatories are overly broad, seek to require more of Plaintiff than any obligation imposed by law, would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense, and would seek to impose upon Plaintiff an obligation to investigate, discover, or produce information or materials from third parties or otherwise that are accessible to Defendant or readily obtainable from public or other sources. Fed. R. Civ. Proc. 26(b)(1), (2).

9. Plaintiff objects to the Interrogatory in its entirety to the extent it seeks information or production of documents protected from disclosure by any right to privacy or any other applicable privilege or protection, including the right to confidentiality or privacy of third parties, any right of confidentiality provided for by Plaintiff's contracts or agreements with such third parties, or by Plaintiff's obligations under applicable law or contract to protect such confidential information. Plaintiff reserves the right to withhold any responsive information or documents

governed by a third-party confidentiality agreement until such time as the appropriate notice can be given or the appropriate permissions can be obtained. Plaintiff also objects generally to all instructions, definitions, or the Interrogatory to the extent it seeks disclosure of trade secrets and other confidential research or analyses, development, or commercial information of Plaintiff or any third party.

10. Plaintiff objects to the Interrogatory in its entirety to the extent it is overbroad and unduly burdensome, particularly to the extent they seek "all," "each," or "any" documents, witnesses, individuals, persons, organizations, statements, or facts that refer or relate to various subject matters. Fed. R. Civ. Proc. 26(b)(1), (2). To the extent Plaintiff responds to the Interrogatory, Plaintiff will use reasonable diligence to identify responsive documents, witnesses, individuals, persons, organizations, statements, or facts in its possession, custody, or control, based on its present knowledge, information, and belief.

11. Plaintiff objects to the Interrogatory in its entirety to the extent it seeks expert discovery prematurely.

12. Plaintiff objects to the Interrogatory in its entirety to the extent it purports to require Plaintiff to restore and/or search data sources that are not reasonably accessible on the grounds that such definitions and Interrogatory would subject Plaintiff to undue burden and expense. Fed. R. Civ. Proc. 26(b)(1), (2).

III. DEFINITIONAL OBJECTIONS.

1. Plaintiff objects to definition number one (1) to the extent it defines "Plaintiff" and "Wikimedia" to include Plaintiff's "parent, subsidiary, and affiliated organizations, and all persons acting on their behalf, including officials, agents, employees, attorneys, and consultants." Said definition is overly broad, seeks irrelevant information not calculated to lead to the discovery of

admissible evidence, seeks information outside Plaintiff's possession, custody, or control, and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden and expense. Said definition is also vague and ambiguous in that it cannot be determined what is meant by the terms "affiliated organizations" and "all persons acting on their behalf." Plaintiff shall construe "Plaintiff" and "Wikimedia" to mean Wikimedia, and its present officers, directors, agents, and employees.

2. Plaintiff objects to the definition of "identify" with respect to Internet Protocol ("IP") addresses because this definition calls for a significant and burdensome collection of information in addition to the IP addresses themselves. The additional information called for by the definition of "identify" is overbroad, unduly burdensome, not proportional and seeks information that is not reasonably calculated to lead to the discovery of admissible evidence relevant to jurisdictional issues.

IV. INSTRUCTIONAL OBJECTIONS

1. Plaintiff objects to instruction number one (1) to the extent it purports to request "knowledge or information" from Wikimedia's "parent, subsidiary, or affiliated organizations, and their officials, agents, employees, attorneys, consultants, and any other person acting on their behalf." Said request is overly broad, seeks irrelevant information not calculated to lead to the discovery of admissible evidence, seeks information outside Plaintiff's possession, custody, or control, and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden and expense. Moreover, said request is vague and ambiguous in that it cannot be determined what is meant by the term "affiliated organizations" and "any other person acting on their behalf." Where an Interrogatory requests knowledge or information of Plaintiff, Plaintiff shall construe such request to mean knowledge or information from Wikimedia, and its present officers, directors,

agents, and employees.

2. Plaintiff objects to instruction number two (2) as unduly burdensome to the extent it imposes an obligation to provide information greater than that required by the Federal Rules of Civil Procedure.

3. Plaintiff objects to instruction number three (3) as unduly burdensome and imposing an obligation to provide information greater than that required by the Federal Rules of Civil Procedure to the extent it purports to require Plaintiff to "identify each person known by Plaintiff to have such knowledge, and in each instance where Plaintiff avers insufficient knowledge or information as a grounds for not providing information or for providing only a portion of the information requested, set forth a description of the efforts made to locate information needed to answer the interrogatory."

4. Plaintiff objects to instruction number four (4) to the extent it seeks to require it to identify anything other than the specific claim of privilege or work product being made and the basis for such claim, and to the extent it seeks to require any information not specified in Discovery Guideline 10, on the grounds that the additional information sought by Defendant would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense, and constitutes information protected from discovery by privilege and as work product. Plaintiff is willing to discuss acceptable reciprocal obligations for disclosure of information withheld on the basis of attorney-client privilege or attorney work-product.

5. Plaintiff objects to instruction number five (5) that the Interrogatory is continuing, to the extent said instruction seeks unilaterally to impose an obligation to provide supplemental information greater than that required by Federal Rule of Civil Procedure 26(e) and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense. Plaintiff will

comply with the requirements of the Federal Rules of Civil Procedure and is willing to discuss mutually acceptable reciprocal obligations for continuing discovery.

V. SPECIFIC OBJECTIONS AND RESPONSE TO INTERROGATORY NO. 19.

Without waiving or limiting in any manner any of the foregoing General Objections, Definitional Objections, or Instructional Objections, but rather incorporating them into the following response to the extent applicable, Plaintiff responds to Defendant's Interrogatory No. 19 as follows:

INTERROGATORY NO. 19:

NSA Interrogatory No. 3 requests that Plaintiff identify each category of Wikimedia international, text-based, Internet communications that Plaintiff contends is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance. For the period January 1, 2017, to the present, please describe the communications in each such category by stating:

> a. each communications protocol used to transmit Wikimedia communications in that category;
>
> b. the number, to the extent it is known or can be estimated, of Wikimedia communications in that category using each protocol;
>
> c. to the extent known, the countries to and from which Wikimedia communications in that category, using each protocol, are transmitted;
>
> d. whether and by what means communications in that category using each type of protocol are encrypted; and
>
> e. the Internet Protocol (IP) addresses or address blocks used by Wikimedia for purposes of transmitting or receiving communications in that category.

If Plaintiff does not intend at summary judgment or trial to offer proof that communications in a given category that use a given protocol are intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, then it need not identify, quantify, or otherwise respond to this interrogatory concerning communications in that category using that protocol.

RESPONSE TO INTERROGATORY NO. 19:

In addition to Plaintiff's General Objections, which are incorporated herein, Plaintiff objects to this Interrogatory because it is improperly compound and contains multiple subparts. Plaintiff also objects that this Interrogatory is vague and ambiguous as to its use of the term "communications protocol." Plaintiff further objects that this Interrogatory is overly broad, unduly burdensome, not proportional and seeks information that is not reasonably calculated to lead to the discovery of admissible evidence relevant to jurisdictional issues. Wikimedia objects to the Interrogatory as unreasonably cumulative and duplicative of Defendants' written discovery requests and Wikimedia's written discovery responses and document productions in this matter, including, *inter alia*, NSA Interrogatory Nos. 6-8 and ODNI Interrogatory Nos. 14-15.

Plaintiff additionally objects to this Interrogatory to the extent that it seeks information that is not within Plaintiff's possession, custody and control or public information that is equally accessible to Defendant. Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and as ordered by the Court. *See* ECF No. 117. For example, to the extent the Interrogatory seeks information concerning the volume or proportion of Wikimedia communications that are encrypted and the encryption protocols used, Wikimedia objects that such subjects exceed the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and as ordered by the Court. *See* ECF No. 117.

On the basis of these General and Specific Objections, Plaintiff will not provide a response to this Interrogatory.

AMENDED RESPONSE TO INTERROGATORY NO. 19:

In addition to Plaintiff's General Objections, which are incorporated herein, Plaintiff objects to this Interrogatory because it is improperly compound and contains multiple subparts. Plaintiff also objects that this Interrogatory is vague and ambiguous as to its use of the term "communications protocol." Plaintiff further objects that this Interrogatory is overly broad, unduly burdensome, not proportional and seeks information that is not reasonably calculated to lead to the discovery of admissible evidence relevant to jurisdictional issues. Wikimedia objects to the Interrogatory as unreasonably cumulative and duplicative of Defendants' written discovery requests and Wikimedia's written discovery responses and document productions in this matter, including, *inter alia*, NSA Interrogatory Nos. 6-8 and ODNI Interrogatory Nos. 14-15.

Plaintiff additionally objects to this Interrogatory to the extent that it seeks information that is not within Plaintiff's possession, custody and control or public information that is equally accessible to Defendant. Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and as ordered by the Court. *See* ECF No. 117. For example, to the extent the Interrogatory seeks information concerning the volume or proportion of Wikimedia communications that are encrypted and the encryption protocols used, Wikimedia objects that such subjects exceed the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and as ordered by the Court. *See* ECF No. 117.

Subject to and without waiving any of these General or Specific Objections, Plaintiff's response to this Interrogatory is contained in the attached Exhibit 1, and Exhibits A–G.

Dated: April 6, 2018

/s/ Ashley Gorski

Ashley Gorski
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
agorski@aclu.org

Counsel for Plaintiff

EXHIBIT 1

TECHNICAL STATISTICS FOR 2017 TO 2018 RESPONSIVE TO ODNI INTERROGATORY NO. 19						
Protocol	**Volume**	**Date Range**	**Foreign Countries, Regions, Territories**	**IP Addresses**	**Encryption Status**	**Additional Notes**
ODNI Interrogatory 19(a)	*ODNI Interrogatory 19(b)*		*ODNI Interrogatory 19(c)*	*ODNI Interrogatory 19(e)*	*ODNI Interrogatory 19(d)*	*ODNI Interrogatory 19 (d)*
Category 1 Wikimedia communications with its community members, who read and contribute to Wikimedia's Projects and webpages, and who use the Projects and webpages to interact with each other						
Total HTTP & HTTPS requests: foreign users to WMF US servers	381,655,849,279	Aug. 1, 2017, to Jan. 31, 2018 (six months)	List of countries for HTTPS (Exhibit A)	198.35.26.0/23, 208.80.152.0/22, 2620:0:860::/48, 2620:0:861::/48, 2620:0:863::/48	HTTPS: 373,045,851,598	For clarity, these HTTPS and HTTP requests use the same IP addresses.
			List of countries for HTTP (Exhibit B)		HTTP: 8,609,997,681	
Total HTTP & HTTPS requests: US users to WMF foreign servers	2,812,819,460	Aug. 1, 2017, to Jan. 31, 2018 (six months)	Netherlands	91.198.174.0/24, 2620:0:862::/48	HTTPS: 2,479,014,613	For clarity, these HTTPS and HTTP requests use the same IP addresses.
					HTTP: 333,804,847	
SMTP communications: foreign users to WMF US servers	Unknown		Unknown	208.80.152.0/22, 2620:0:860::/48, 2620:0:861::/48	Unknown	
Category 2 Wikimedia's internal log communications						
Apache Kafka log communications transmitted from WMF foreign servers to WMF US servers	736,045,377,450	Aug. 1, 2017, to Jan. 31, 2018 (six months)	Netherlands	10.0 0 0/8, 2620:0:860: /46	736,045,377,450 log communications encrypted using IPSec	
Category 3 Communications by Wikimedia staff						
Logged international TCP connections using WMF Office Network or WMF VPN	4,948,011	Mar. 1, 2017 to Feb. 28, 2018 (one year)	List of countries for non-VPN (Exhibit C); List of countries for VPN (Exhibit D)	The WMF Office Network IP range is 198.73.209 0/24, with the WMF VPN operating on IP address 198.73.209 25	All 791 connections encrypted using OpenVPN (SSL/TLS protocol)	Other than the VPN connections, Wikimedia itself does not systematically encrypt connections to and from the office network router and it would not be practical for it to do so. However, individuals who use the office network router may establish encrypted connections based on the particular communications services they use at any given time. Because Wikimedia's office network router does not log application-layer protocol information, Wikimedia does not know with certainty the extent to which the data transmitted over these non-VPN connections is encrypted. The logs do contain, however, the source and destination ports of connections, which in certain cases may shed light on the encryption status of connections, such as those that use port 443 or port 22.

Logged international UDP connections using WMF Office Network or WMF VPN	2,207,771	Mar. 1, 2017 to Feb. 28, 2018 (one year)	List of countries for non-VPN (Exhibit E); List of countries for VPN (Exhibit F)	The WMF Office Network IP range is 198.73.209 0/24, with the WMF VPN operating on IP address 198.73.209 25	All 19,709 connections encrypted using OpenVPN (SSL/TLS protocol)	Same response.
Logged international ICMP connections using WMF Office Network or WMF VPN	51,301	Mar. 1, 2017 to Feb. 28, 2018 (one year)	List of countries for non-VPN (Exhibit G)	The WMF Office Network IP range is 198.73.209 0/24, with the WMF VPN operating on IP address 198.73.209 25	0 connections encrypted using VPN	Same response.

EXHIBIT A

List of Countries with HTTPS Requests to Wikimedia Servers in United States from August 1, 2017 to January 31, 2018

1.	Afghanistan
2.	Åland
3.	Albania
4.	Algeria
5.	Andorra
6.	Angola
7.	Anguilla
8.	Antigua and Barbuda
9.	Argentina
10.	Armenia
11.	Aruba
12.	Australia
13.	Austria
14.	Azerbaijan
15.	Bahamas
16.	Bahrain
17.	Bangladesh
18.	Barbados
19.	Belarus
20.	Belgium
21.	Belize
22.	Benin
23.	Bermuda
24.	Bhutan
25.	Bolivia
26.	Bonaire, Sint Eustatius, and Saba
27.	Bosnia and Herzegovina
28.	Botswana
29.	Brazil
30.	British Indian Ocean Territory
31.	British Virgin Islands
32.	Brunei
33.	Bulgaria
34.	Burkina Faso
35.	Burundi
36.	Cabo Verde
37.	Cambodia
38.	Cameroon
39.	Canada
40.	Cayman Islands

41.	Central African Republic
42.	Chad
43.	Chile
44.	China
45.	Christmas Island
46.	Cocos [Keeling] Islands
47.	Colombia
48.	Comoros
49.	Congo
50.	Cook Islands
51.	Costa Rica
52.	Croatia
53.	Cuba
54.	Curaçao
55.	Cyprus
56.	Czechia
57.	Denmark
58.	Djibouti
59.	Dominica
60.	Dominican Republic
61.	East Timor
62.	Ecuador
63.	Egypt
64.	El Salvador
65.	Equatorial Guinea
66.	Eritrea
67.	Estonia
68.	Ethiopia
69.	Falkland Islands
70.	Faroe Islands
71.	Federated States of Micronesia
72.	Fiji
73.	Finland
74.	France
75.	French Guiana
76.	French Polynesia
77.	French Southern Territories
78.	Gabon
79.	Gambia
80.	Georgia
81.	Germany
82.	Ghana
83.	Gibraltar

84.	Greece
85.	Greenland
86.	Grenada
87.	Guadeloupe
88.	Guatemala
89.	Guernsey
90.	Guinea
91.	Guinea-Bissau
92.	Guyana
93.	Haiti
94.	Hashemite Kingdom of Jordan
95.	Honduras
96.	Hong Kong
97.	Hungary
98.	Iceland
99.	India
100.	Indonesia
101.	Iran
102.	Iraq
103.	Ireland
104.	Isle of Man
105.	Israel
106.	Italy
107.	Ivory Coast
108.	Jamaica
109.	Japan
110.	Jersey
111.	Kazakhstan
112.	Kenya
113.	Kiribati
114.	Kosovo
115.	Kuwait
116.	Kyrgyzstan
117.	Laos
118.	Latvia
119.	Lebanon
120.	Lesotho
121.	Liberia
122.	Libya
123.	Liechtenstein
124.	Luxembourg
125.	Macao
126.	Macedonia

127.	Madagascar
128.	Malawi
129.	Malaysia
130.	Maldives
131.	Mali
132.	Malta
133.	Marshall Islands
134.	Martinique
135.	Mauritania
136.	Mauritius
137.	Mayotte
138.	Mexico
139.	Monaco
140.	Mongolia
141.	Montenegro
142.	Montserrat
143.	Morocco
144.	Mozambique
145.	Myanmar [Burma]
146.	Namibia
147.	Nauru
148.	Nepal
149.	Netherlands
150.	New Caledonia
151.	New Zealand
152.	Nicaragua
153.	Niger
154.	Nigeria
155.	Niue
156.	Norfolk Island
157.	North Korea
158.	Norway
159.	Oman
160.	Pakistan
161.	Palau
162.	Palestine
163.	Panama
164.	Papua New Guinea
165.	Paraguay
166.	Peru
167.	Philippines
168.	Pitcairn Islands
169.	Poland

170.	Portugal
171.	Qatar
172.	Republic of Korea
173.	Republic of Lithuania
174.	Republic of Moldova
175.	Republic of the Congo
176.	Romania
177.	Russia
178.	Rwanda
179.	Réunion
180.	Saint Helena
181.	Saint Kitts and Nevis
182.	Saint Lucia
183.	Saint Martin
184.	Saint Pierre and Miquelon
185.	Saint Vincent and the Grenadines
186.	Saint Barthélemy
187.	Samoa
188.	San Marino
189.	Saudi Arabia
190.	Senegal
191.	Serbia
192.	Seychelles
193.	Sierra Leone
194.	Singapore
195.	Sint Maarten
196.	Slovak Republic
197.	Slovakia
198.	Slovenia
199.	Solomon Islands
200.	Somalia
201.	South Africa
202.	South Georgia and the South Sandwich Islands
203.	South Sudan
204.	Spain
205.	Sri Lanka
206.	St Kitts and Nevis
207.	Sudan
208.	Suriname
209.	Svalbard and Jan Mayen
210.	Swaziland
211.	Sweden

212.	Switzerland
213.	Syria
214.	São Tomé and Príncipe
215.	Taiwan
216.	Tajikistan
217.	Tanzania
218.	Thailand
219.	Togo
220.	Tokelau
221.	Tonga
222.	Trinidad and Tobago
223.	Tunisia
224.	Turkey
225.	Turkmenistan
226.	Turks and Caicos Islands
227.	Tuvalu
228.	Uganda
229.	Ukraine
230.	United Arab Emirates
231.	United Kingdom
232.	Uruguay
233.	Uzbekistan
234.	Vanuatu
235.	Vatican City
236.	Venezuela
237.	Vietnam
238.	Wallis and Futuna
239.	Western Sahara
240.	Yemen
241.	Zambia
242.	Zimbabwe

EXHIBIT B

List of Countries with HTTP Requests to Wikimedia Servers in United States from August 1, 2017 to January 31, 2018

1.	Afghanistan
2.	Åland
3.	Albania
4.	Algeria
5.	Andorra
6.	Angola
7.	Anguilla
8.	Antigua and Barbuda
9.	Argentina
10.	Armenia
11.	Aruba
12.	Australia
13.	Austria
14.	Azerbaijan
15.	Bahamas
16.	Bahrain
17.	Bangladesh
18.	Barbados
19.	Belarus
20.	Belgium
21.	Belize
22.	Benin
23.	Bermuda
24.	Bhutan
25.	Bolivia
26.	Bonaire, Sint Eustatius, and Saba
27.	Bosnia and Herzegovina
28.	Botswana
29.	Brazil
30.	British Indian Ocean Territory
31.	British Virgin Islands
32.	Brunei
33.	Bulgaria
34.	Burkina Faso
35.	Burundi
36.	Cabo Verde
37.	Cambodia
38.	Cameroon
39.	Canada
40.	Cayman Islands

41.	Central African Republic
42.	Chad
43.	Chile
44.	China
45.	Christmas Island
46.	Cocos [Keeling] Islands
47.	Colombia
48.	Comoros
49.	Congo
50.	Cook Islands
51.	Costa Rica
52.	Croatia
53.	Cuba
54.	Curaçao
55.	Cyprus
56.	Czechia
57.	Denmark
58.	Djibouti
59.	Dominica
60.	Dominican Republic
61.	East Timor
62.	Ecuador
63.	Egypt
64.	El Salvador
65.	Equatorial Guinea
66.	Eritrea
67.	Estonia
68.	Ethiopia
69.	Falkland Islands
70.	Faroe Islands
71.	Federated States of Micronesia
72.	Fiji
73.	Finland
74.	France
75.	French Guiana
76.	French Polynesia
77.	French Southern Territories
78.	Gabon
79.	Gambia
80.	Georgia
81.	Germany
82.	Ghana
83.	Gibraltar

84.	Greece
85.	Greenland
86.	Grenada
87.	Guadeloupe
88.	Guatemala
89.	Guernsey
90.	Guinea
91.	Guinea-Bissau
92.	Guyana
93.	Haiti
94.	Hashemite Kingdom of Jordan
95.	Honduras
96.	Hong Kong
97.	Hungary
98.	Iceland
99.	India
100.	Indonesia
101.	Iran
102.	Iraq
103.	Ireland
104.	Isle of Man
105.	Israel
106.	Italy
107.	Ivory Coast
108.	Jamaica
109.	Japan
110.	Jersey
111.	Kazakhstan
112.	Kenya
113.	Kiribati
114.	Kosovo
115.	Kuwait
116.	Kyrgyzstan
117.	Laos
118.	Latvia
119.	Lebanon
120.	Lesotho
121.	Liberia
122.	Libya
123.	Liechtenstein
124.	Luxembourg
125.	Macao
126.	Macedonia

127.	Madagascar
128.	Malawi
129.	Malaysia
130.	Maldives
131.	Mali
132.	Malta
133.	Marshall Islands
134.	Martinique
135.	Mauritania
136.	Mauritius
137.	Mayotte
138.	Mexico
139.	Monaco
140.	Mongolia
141.	Montenegro
142.	Montserrat
143.	Morocco
144.	Mozambique
145.	Myanmar [Burma]
146.	Namibia
147.	Nauru
148.	Nepal
149.	Netherlands
150.	New Caledonia
151.	New Zealand
152.	Nicaragua
153.	Niger
154.	Nigeria
155.	Niue
156.	Norfolk Island
157.	North Korea
158.	Norway
159.	Oman
160.	Pakistan
161.	Palau
162.	Palestine
163.	Panama
164.	Papua New Guinea
165.	Paraguay
166.	Peru
167.	Philippines
168.	Pitcairn Islands
169.	Poland

170.	Portugal
171.	Qatar
172.	Republic of Korea
173.	Republic of Lithuania
174.	Republic of Moldova
175.	Republic of the Congo
176.	Romania
177.	Russia
178.	Rwanda
179.	Réunion
180.	Saint Helena
181.	Saint Kitts and Nevis
182.	Saint Lucia
183.	Saint Martin
184.	Saint Pierre and Miquelon
185.	Saint Vincent and the Grenadines
186.	Saint Barthélemy
187.	Samoa
188.	San Marino
189.	Saudi Arabia
190.	Senegal
191.	Serbia
192.	Seychelles
193.	Sierra Leone
194.	Singapore
195.	Sint Maarten
196.	Slovak Republic
197.	Slovakia
198.	Slovenia
199.	Solomon Islands
200.	Somalia
201.	South Africa
202.	South Georgia and the South Sandwich Islands
203.	South Sudan
204.	Spain
205.	Sri Lanka
206.	St Kitts and Nevis
207.	Sudan
208.	Suriname
209.	Svalbard and Jan Mayen
210.	Swaziland
211.	Sweden

212.	Switzerland
213.	Syria
214.	São Tomé and Príncipe
215.	Taiwan
216.	Tajikistan
217.	Tanzania
218.	Thailand
219.	Togo
220.	Tokelau
221.	Tonga
222.	Trinidad and Tobago
223.	Tunisia
224.	Turkey
225.	Turkmenistan
226.	Turks and Caicos Islands
227.	Tuvalu
228.	Uganda
229.	Ukraine
230.	United Arab Emirates
231.	United Kingdom
232.	Uruguay
233.	Uzbekistan
234.	Vanuatu
235.	Vatican City
236.	Venezuela
237.	Vietnam
238.	Wallis and Futuna
239.	Western Sahara
240.	Yemen
241.	Zambia
242.	Zimbabwe

EXHIBIT C

List of Countries with Logged non-VPN TCP Connections to Wikimedia Office Router in United States from March 1, 2017 to February 28, 2018

1.	Andorra
2.	United Arab Emirates
3.	Afghanistan
4.	Antigua and Barbuda
5.	Albania
6.	Armenia
7.	Angola
8.	Antarctica
9.	Argentina
10.	Austria
11.	Australia
12.	Aruba
13.	Aland Islands
14.	Azerbaijan
15.	Bosnia and Herzegovina
16.	Barbados
17.	Bangladesh
18.	Belgium
19.	Burkina Faso
20.	Bulgaria
21.	Bahrain
22.	Burundi
23.	Benin
24.	Saint Bartelemey
25.	Bermuda
26.	Brunei Darussalam
27.	Bolivia
28.	Bonaire, Saint Eustatius and Saba
29.	Brazil
30.	Bahamas
31.	Bhutan
32.	Botswana
33.	Belarus
34.	Belize
35.	Canada
36.	Congo, The Democratic Republic of the
37.	Central African Republic
38.	Congo
39.	Switzerland
40.	Cote d'Ivoire

41.	Cook Islands
42.	Chile
43.	Cameroon
44.	China
45.	Colombia
46.	Costa Rica
47.	Cuba
48.	Cape Verde
49.	Curacao
50.	Christmas Island
51.	Cyprus
52.	Czech Republic
53.	Germany
54.	Djibouti
55.	Denmark
56.	Dominica
57.	Dominican Republic
58.	Algeria
59.	Ecuador
60.	Estonia
61.	Egypt
62.	Eritrea
63.	Spain
64.	Ethiopia
65.	Europe
66.	Finland
67.	Fiji
68.	France
69.	Gabon
70.	United Kingdom
71.	Grenada
72.	Georgia
73.	French Guiana
74.	Guernsey
75.	Ghana
76.	Gibraltar
77.	Greenland
78.	Gambia
79.	Guadeloupe
80.	Equatorial Guinea
81.	Greece
82.	Guatemala
83.	Guam

84.	Guyana
85.	Hong Kong
86.	Honduras
87.	Croatia
88.	Haiti
89.	Hungary
90.	Indonesia
91.	Ireland
92.	Israel
93.	Isle of Man
94.	India
95.	Iraq
96.	Iran, Islamic Republic of
97.	Iceland
98.	Italy
99.	Jersey
100.	Jamaica
101.	Jordan
102.	Japan
103.	Kenya
104.	Kyrgyzstan
105.	Cambodia
106.	Kiribati
107.	Comoros
108.	Saint Kitts and Nevis
109.	Korea, Democratic People's Republic of
110.	Korea, Republic of
111.	Kuwait
112.	Cayman Islands
113.	Kazakhstan
114.	Lao People's Democratic Republic
115.	Lebanon
116.	Saint Lucia
117.	Liechtenstein
118.	Sri Lanka
119.	Liberia
120.	Lesotho
121.	Lithuania
122.	Luxembourg
123.	Latvia
124.	Libyan Arab Jamahiriya
125.	Morocco
126.	Monaco

127.	Moldova, Republic of
128.	Montenegro
129.	Saint Martin
130.	Madagascar
131.	Marshall Islands
132.	Macedonia
133.	Mali
134.	Myanmar
135.	Mongolia
136.	Macao
137.	Northern Mariana Islands
138.	Martinique
139.	Mauritania
140.	Malta
141.	Mauritius
142.	Maldives
143.	Malawi
144.	Mexico
145.	Malaysia
146.	Mozambique
147.	Namibia
148.	New Caledonia
149.	Niger
150.	Nigeria
151.	Nicaragua
152.	Netherlands
153.	Norway
154.	Nepal
155.	New Zealand
156.	Oman
157.	Panama
158.	Peru
159.	French Polynesia
160.	Papua New Guinea
161.	Philippines
162.	Pakistan
163.	Poland
164.	Puerto Rico
165.	Palestinian Territory
166.	Portugal
167.	Palau
168.	Paraguay
169.	Qatar

170.	Reunion
171.	Romania
172.	Serbia
173.	Russian Federation
174.	Rwanda
175.	Saudi Arabia
176.	Solomon Islands
177.	Seychelles
178.	Sudan
179.	Sweden
180.	Singapore
181.	Slovenia
182.	Slovakia
183.	Sierra Leone
184.	Senegal
185.	Somalia
186.	Suriname
187.	South Sudan
188.	Sao Tome and Principe
189.	El Salvador
190.	Sint Maarten
191.	Syrian Arab Republic
192.	Swaziland
193.	Turks and Caicos Islands
194.	Chad
195.	Togo
196.	Thailand
197.	Tajikistan
198.	Turkmenistan
199.	Tunisia
200.	Tonga
201.	Turkey
202.	Trinidad and Tobago
203.	Taiwan
204.	Tanzania, United Republic of
205.	Ukraine
206.	Uganda
207.	Uruguay
208.	Uzbekistan
209.	Holy See (Vatican City State)
210.	Saint Vincent and the Grenadines
211.	Venezuela
212.	Virgin Islands, British

213.	Virgin Islands, U.S.
214.	Vietnam
215.	Vanuatu
216.	Samoa
217.	Kosovo
218.	Yemen
219.	South Africa
220.	Zambia
221.	Zimbabwe

EXHIBIT D

List of Countries with Logged VPN TCP Connections to Wikimedia Office Router in United States from March 1, 2017 to February 28, 2018

1.	United Arab Emirates
2.	Bulgaria
3.	Brazil
4.	Canada
5.	Switzerland
6.	China
7.	Colombia
8.	Germany
9.	Spain
10.	France
11.	United Kingdom
12.	Greece
13.	Hong Kong
14.	Ireland
15.	Iceland
16.	Japan
17.	Korea, Republic of
18.	Latvia
19.	Moldova, Republic of
20.	Mongolia
21.	Nigeria
22.	Netherlands
23.	Portugal
24.	Romania
25.	Russian Federation
26.	Seychelles
27.	Singapore
28.	Ukraine
29.	Uzbekistan

EXHIBIT E

List of Countries with Logged non-VPN UDP Connections to Wikimedia Office Router in United States from March 1, 2017 to February 28, 2018

1.	United Arab Emirates
2.	Antigua and Barbuda
3.	Anguilla
4.	Albania
5.	Armenia
6.	Angola
7.	Antarctica
8.	Argentina
9.	Austria
10.	Australia
11.	Aruba
12.	Aland Islands
13.	Azerbaijan
14.	Bosnia and Herzegovina
15.	Barbados
16.	Bangladesh
17.	Belgium
18.	Burkina Faso
19.	Bulgaria
20.	Bahrain
21.	Burundi
22.	Benin
23.	Bermuda
24.	Brunei Darussalam
25.	Bolivia
26.	Bonaire, Saint Eustatius and Saba
27.	Brazil
28.	Bahamas
29.	Bhutan
30.	Botswana
31.	Belarus
32.	Belize
33.	Canada
34.	Switzerland
35.	Cote d'Ivoire
36.	Cook Islands
37.	Chile
38.	Cameroon
39.	China
40.	Colombia

41.	Costa Rica
42.	Cuba
43.	Cape Verde
44.	Curacao
45.	Cyprus
46.	Czech Republic
47.	Germany
48.	Denmark
49.	Dominica
50.	Dominican Republic
51.	Algeria
52.	Ecuador
53.	Estonia
54.	Egypt
55.	Spain
56.	Ethiopia
57.	Europe
58.	Finland
59.	Fiji
60.	France
61.	Gabon
62.	United Kingdom
63.	Grenada
64.	Georgia
65.	French Guiana
66.	Guernsey
67.	Ghana
68.	Gibraltar
69.	Greenland
70.	Guinea
71.	Guadeloupe
72.	Greece
73.	Guatemala
74.	Guam
75.	Guyana
76.	Hong Kong
77.	Honduras
78.	Croatia
79.	Hungary
80.	Indonesia
81.	Ireland
82.	Israel
83.	Isle of Man

84.	India
85.	Iraq
86.	Iran, Islamic Republic of
87.	Iceland
88.	Italy
89.	Jersey
90.	Jamaica
91.	Jordan
92.	Japan
93.	Kenya
94.	Kyrgyzstan
95.	Cambodia
96.	Comoros
97.	Saint Kitts and Nevis
98.	Korea, Democratic People's Republic of
99.	Korea, Republic of
100.	Kuwait
101.	Cayman Islands
102.	Kazakhstan
103.	Lao People's Democratic Republic
104.	Lebanon
105.	Saint Lucia
106.	Liechtenstein
107.	Sri Lanka
108.	Lithuania
109.	Luxembourg
110.	Latvia
111.	Libyan Arab Jamahiriya
112.	Morocco
113.	Monaco
114.	Moldova, Republic of
115.	Montenegro
116.	Saint Martin
117.	Madagascar
118.	Macedonia
119.	Myanmar
120.	Mongolia
121.	Macao
122.	Martinique
123.	Mauritania
124.	Montserrat
125.	Malta
126.	Mauritius

127.	Maldives
128.	Malawi
129.	Mexico
130.	Malaysia
131.	Mozambique
132.	Namibia
133.	New Caledonia
134.	Niger
135.	Nigeria
136.	Nicaragua
137.	Netherlands
138.	Norway
139.	Nepal
140.	Nauru
141.	New Zealand
142.	Oman
143.	Panama
144.	Peru
145.	French Polynesia
146.	Philippines
147.	Pakistan
148.	Poland
149.	Puerto Rico
150.	Palestinian Territory
151.	Portugal
152.	Paraguay
153.	Qatar
154.	Reunion
155.	Romania
156.	Serbia
157.	Russian Federation
158.	Rwanda
159.	Saudi Arabia
160.	Seychelles
161.	Sudan
162.	Sweden
163.	Singapore
164.	Slovenia
165.	Slovakia
166.	Sierra Leone
167.	San Marino
168.	Senegal
169.	Somalia

170.	Suriname
171.	El Salvador
172.	Sint Maarten
173.	Syrian Arab Republic
174.	Swaziland
175.	Turks and Caicos Islands
176.	Chad
177.	Togo
178.	Thailand
179.	Tajikistan
180.	Tokelau
181.	Turkmenistan
182.	Tunisia
183.	Turkey
184.	Trinidad and Tobago
185.	Taiwan
186.	Tanzania, United Republic of
187.	Ukraine
188.	Uganda
189.	Uruguay
190.	Uzbekistan
191.	Holy See (Vatican City State)
192.	Saint Vincent and the Grenadines
193.	Venezuela
194.	Virgin Islands, British
195.	Virgin Islands, U.S.
196.	Vietnam
197.	Vanuatu
198.	Kosovo
199.	Yemen
200.	Mayotte
201.	South Africa
202.	Zambia
203.	Zimbabwe

EXHIBIT F

List of Countries with Logged VPN UDP Connections to Wikimedia Office Router in United States from March 1, 2017 to February 28, 2018

1.	Argentina
2.	Austria
3.	Australia
4.	Canada
5.	China
6.	Colombia
7.	Czech Republic
8.	Germany
9.	Denmark
10.	Egypt
11.	Spain
12.	France
13.	United Kingdom
14.	Greece
15.	Hungary
16.	Iran, Islamic Republic of
17.	Jordan
18.	Mexico
19.	Netherlands
20.	New Zealand
21.	Peru
22.	Poland
23.	Russian Federation
24.	Seychelles
25.	Sweden
26.	Turkey
27.	Uzbekistan

EXHIBIT G

List of Countries with Logged non-VPN ICMP Connections to Wikimedia Office Router in United States from August 1, 2017 to January 31, 2018

1.	United Arab Emirates
2.	Albania
3.	Armenia
4.	Argentina
5.	Austria
6.	Australia
7.	Azerbaijan
8.	Bosnia and Herzegovina
9.	Bangladesh
10.	Belgium
11.	Bulgaria
12.	Bolivia
13.	Brazil
14.	Belarus
15.	Canada
16.	Switzerland
17.	Chile
18.	China
19.	Colombia
20.	Costa Rica
21.	Czech Republic
22.	Germany
23.	Denmark
24.	Dominican Republic
25.	Ecuador
26.	Estonia
27.	Egypt
28.	Spain
29.	Europe
30.	Finland
31.	France
32.	United Kingdom
33.	Georgia
34.	Ghana
35.	Greece
36.	Guatemala
37.	Hong Kong
38.	Croatia
39.	Hungary
40.	Indonesia

41.	Ireland
42.	Israel
43.	India
44.	Iran, Islamic Republic of
45.	Iceland
46.	Italy
47.	Jordan
48.	Japan
49.	Kenya
50.	Kyrgyzstan
51.	Cambodia
52.	Korea, Republic of
53.	Kuwait
54.	Kazakhstan
55.	Lao People's Democratic Republic
56.	Lebanon
57.	Sri Lanka
58.	Lithuania
59.	Luxembourg
60.	Latvia
61.	Morocco
62.	Moldova, Republic of
63.	Macedonia
64.	Mongolia
65.	Mauritius
66.	Mexico
67.	Malaysia
68.	Mozambique
69.	New Caledonia
70.	Netherlands
71.	Norway
72.	Nepal
73.	New Zealand
74.	Peru
75.	French Polynesia
76.	Philippines
77.	Pakistan
78.	Poland
79.	Portugal
80.	Romania
81.	Serbia
82.	Russian Federation
83.	Rwanda

84.	Saudi Arabia
85.	Seychelles
86.	Sudan
87.	Sweden
88.	Singapore
89.	Slovenia
90.	Slovakia
91.	El Salvador
92.	Thailand
93.	Tunisia
94.	Turkey
95.	Taiwan
96.	Tanzania, United Republic of
97.	Ukraine
98.	Uruguay
99.	Uzbekistan
100.	Venezuela
101.	Vietnam
102.	Vanuatu
103.	Kosovo
104.	South Africa
105.	Zimbabwe

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix C

Next Generation Network, and Transoceanic Subsea Cable Updates

Presented by:
City of Virginia Beach
Department of Information Technology
October 4, 2017

City of Virginia Beach Information Technology

Strategic Planning & Partnerships

➢ Master Technology Plan

- A roadmap for how the IT department will partner with other city departments to implement the right technologies needed for long-term business success.

- Includes four major pillars that all IT department initiatives support:
  1. Transforming service delivery
  2. Building better business solutions
  3. Strengthening IT governance
  4. Improving infrastructure and operations

- Next Generation Network (NGN) – Initiative I-1
  - The "Improving infrastructure and operations" pillar included a recommendation to explore ways to create a Next Generation Network.
    - Documents the city's progress in creating the NGN
    - Assesses the city's need and market for future NGN capabilities
    - Provides strategic and technical recommendations for achieving the city's goals related to broadband infrastructure and operations

➢ Broadband Resolution

- Adopted by City Council in March 2015
- Charged staff to explore and create opportunities to leverage NGN investments made by the city and VBCPS to advance high-speed broadband across the region.
- Broad Band Task Force (2015-2016)

Strategic Planning & Partnerships for Next Generation Network

CVB Broadband Task Force Goals

- Purpose and Objective: Build a Next Generation Network that:
  - Provides excellent city services
  - Reduce digital divide for families and businesses
  - Grow our economy
  - Support 21st century jobs
  - Expand fiber network to connect additional off-campus locations to municipal campus and create network redundancy
  - Leverage NGN for the following:
    - Expand educational opportunities
    - Contribute to regional opportunities
    - Utilize “Dig Once” strategy for road and utility projects to include fiber and conduit

CVB Broadband Strategy

- Support city council goal of a financially sustainable city that provides excellent services by making strategic investments in NGN and Transoceanic Cable.
- Create a Middle Mile infrastructure that enhances opportunities in economic development, education, and regional connectivity.
- Enhance the build out new businesses and growth areas (e.g., Biomed) and make business parks fiber ready to attract new businesses.
- Lease excess capacity (dark fiber) vs. providing lit services to create opportunities for expanding internal government services.
- Create internal and external partnerships to take advantage of Transoceanic Cable opportunities.

Regional CIO Broadband Task Force

- City Manager and CIO met regularly with regional City Managers to discuss regional broadband opportunities.
- Collaborated with other municipalities to explore potential regional broadband opportunities.
- Shared education of emerging clusters.

City Manager’s Directive

- Directive to include fiber expansion in all Public Works construction projects.

Strategic Planning & Partnerships for Next Generation Network

- **Broadband White Paper**
  - A High-Speed Broadband White Paper was developed to:
    - Provide a history of broadband on a local, state and national level
    - Identify the current trends in broadband
    - Provide an overview of the laws surrounding broadband
    - Support the city's broadband vision for Virginia Beach, as outlined in the Envision Virginia Beach 2040 report:
      - "Citizens, businesses and visitors have access to advanced broadband technologies that efficiently and effectively supports regional interconnectivity as well as global commerce."
    - Meet market demand

- **Business Case**
  - A business case was developed to provide a financial analysis and comparison between leased network fiber and City-owned network fiber.
  - This document assisted city leadership and stakeholders with determining if the project would provide value to the enterprise.
  - The document also served to justify the capital outlay for the project.
  - Stakeholders from various departments were involved with the assessment of current and future bandwith needs.
  - Costs and savings were identified and entered into a ROI calculator to provide the quantitative benefits of implementing fiber.

- **Formalized Process for Fiber Provisioning Management**
  - Document that describes the processes that will be required for building out the fiber infrastructure
    1. Provisioning fiber to a building location that is not part of the NGN
    2. Provisioning fiber to a building that is being newly constructed by Public Works
    3. Provisioning fiber for road, sidewalk and Intelligent Traffic System projects
    4. Repairing a confirmed fiber service outage
    5. Repairing damaged NGN network infrastructure

Strategic Planning & Partnerships for Next Generation Network

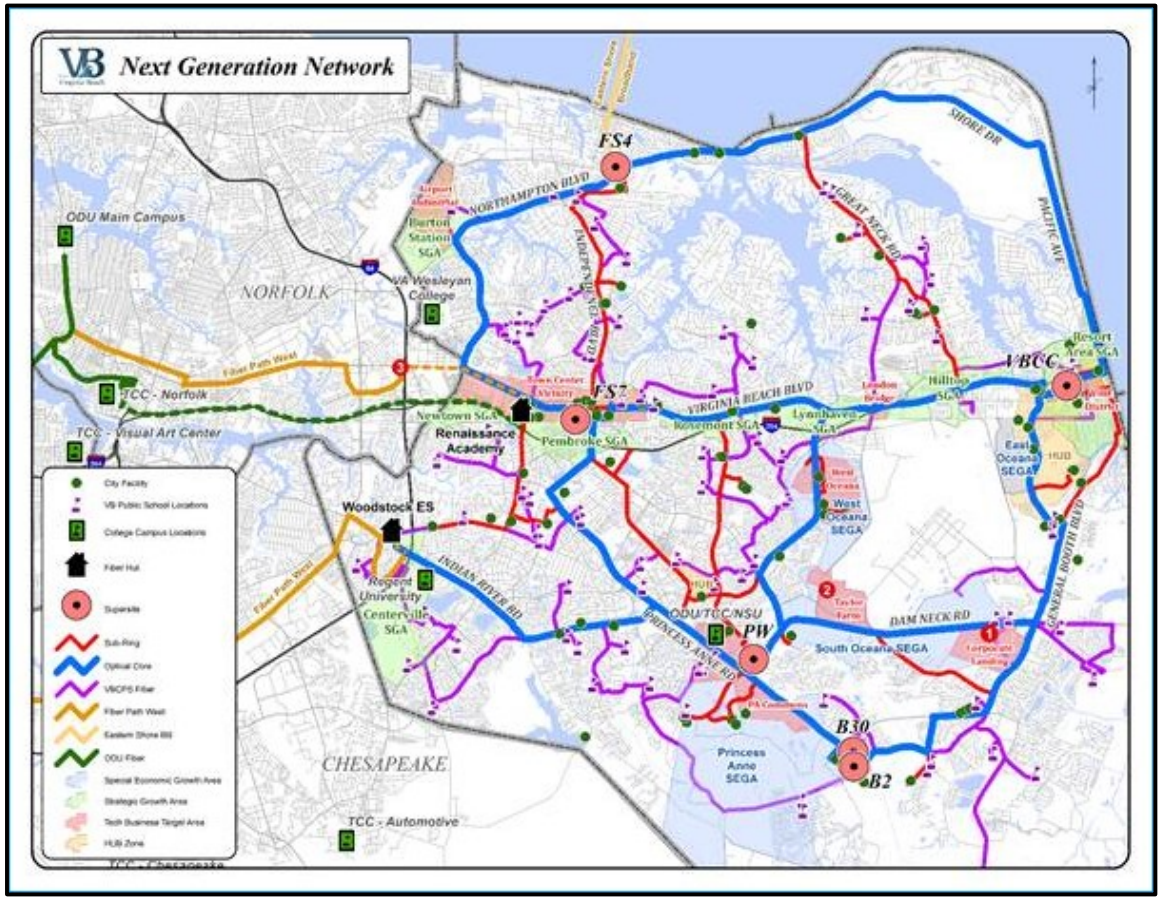
- **CBG Communications**
  - Telecommunications and cable television consulting firm that conducted both residential and business broadband surveys to gauge the community's need for broadband services.

- **3U Technologies**
  - International business consulting, project management and engineering services firm that developed a Proposal for Support of Submarine Cable Landing

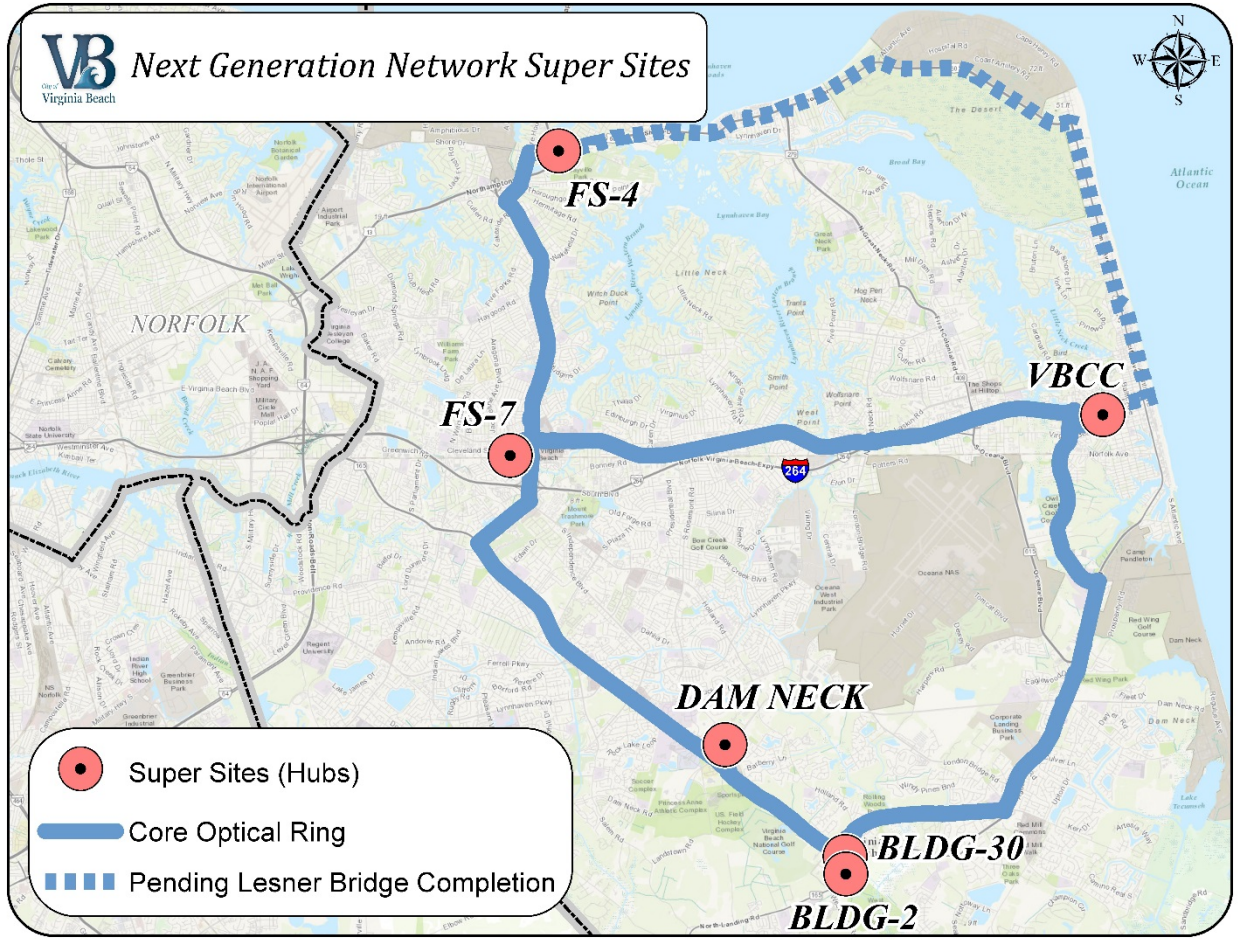
- **CTC Technology & Energy**
  - An independent communications and IT engineering consulting firm that assisted with developing middle mile leasing strategies.

Next Generation Network Buildout

- City of Virginia Beach invested $4.1 million in their FY 15 budget
- Leveraged the existing infrastructure to buildout and connect facilities
- Mapped strategic routes to 60 connected locations
  - Designed for future economic opportunities
  - Taking into consideration the proximity of corporate parks
  - City road projects will include conduit/fiber
  - Put infrastructure in place to support NGN



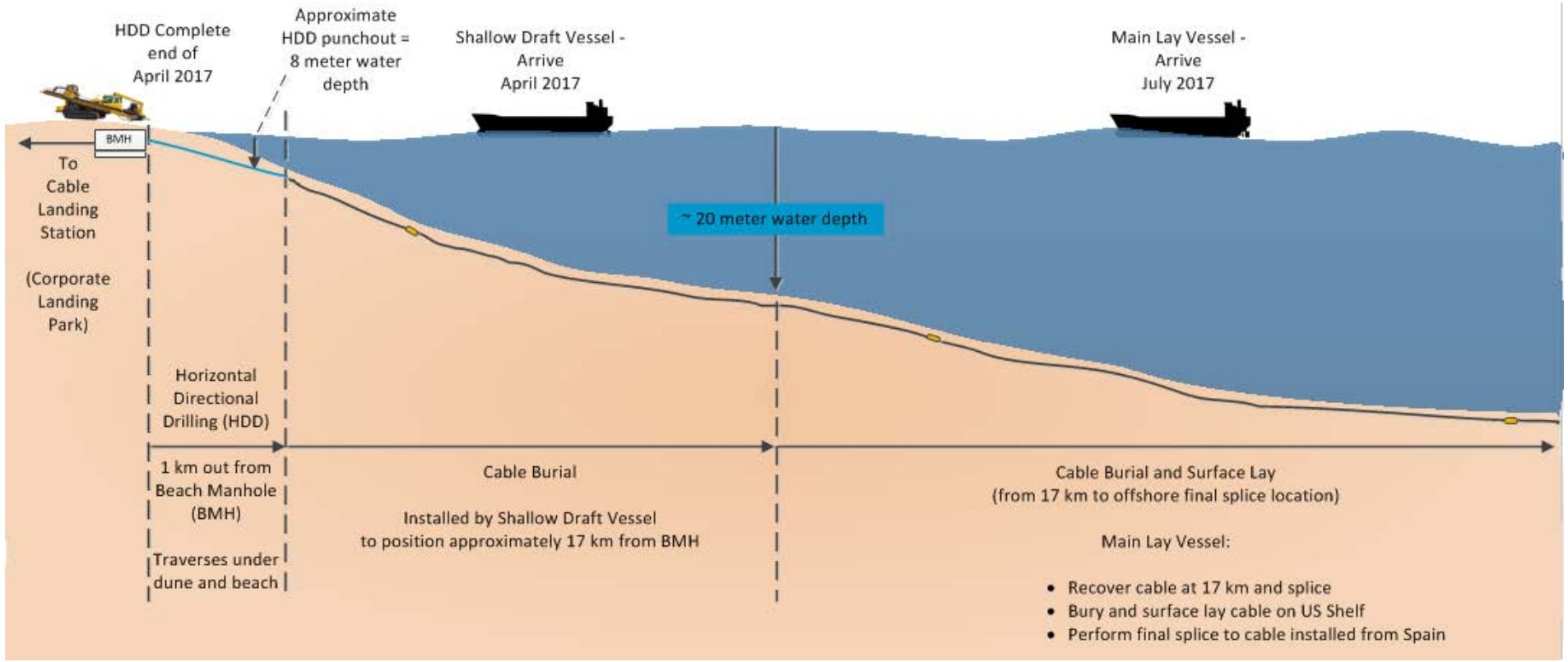
Next Generation Network



- Total of 6 Optical/Super Sites (Phase 0) and
- 54 Remote Locations (Phases 1 through 4)
- Construction Completion Dates:
  - Phase 0 – 06/24/2016
  - Phase 1 – 10/18/2016
  - Phase 2 – 04/07/2017
  - Phase 3 – 04/28/2017
  - Phase 4 – 06/15/2017
- NGN Go Live Date – Dec, 2017

MAREA Cable – From beach to manhole

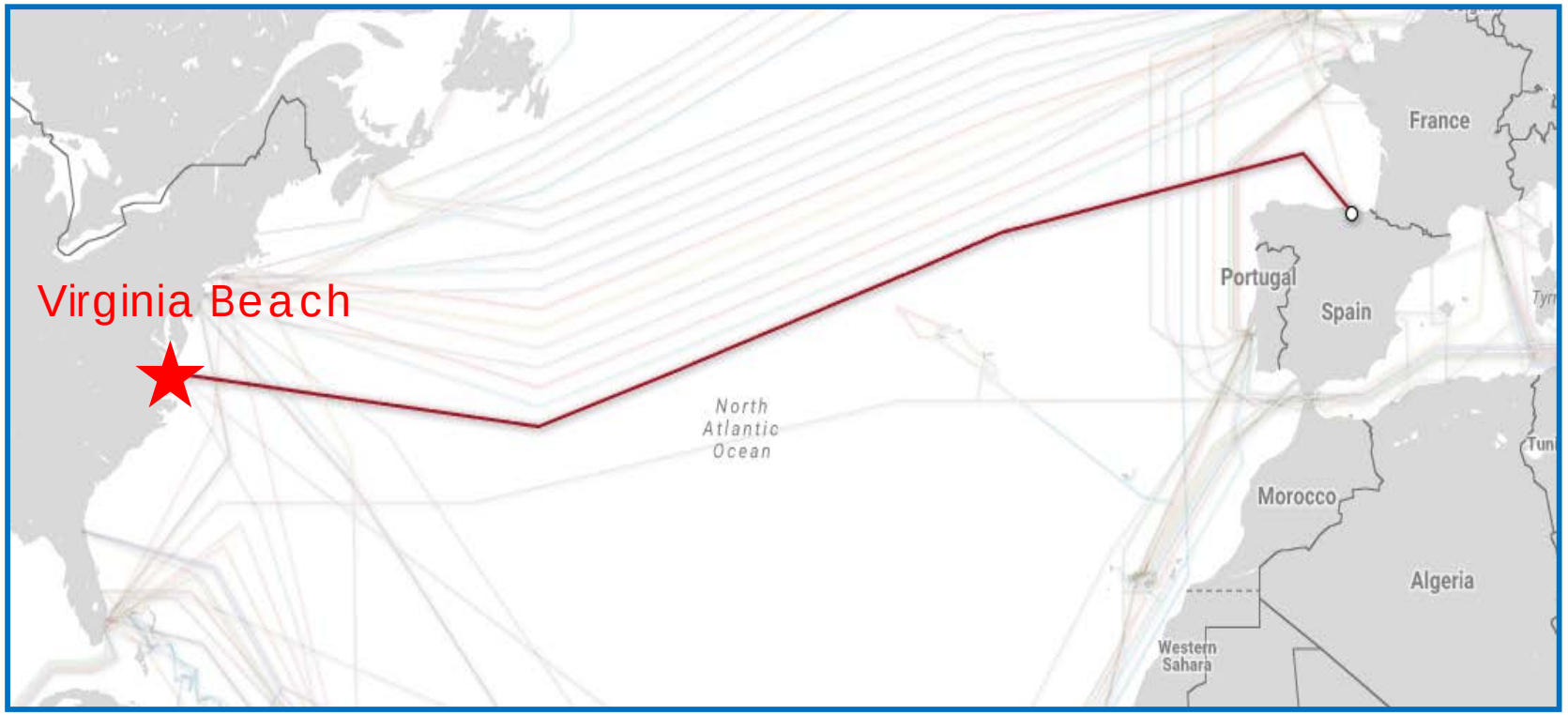
- **Oceanic** Infrastructure connection of subsea cable
  - Will connect sub-sea cable to off-shore duct duckbill flap (4 conduits for the MAREA/BRUSA beach manhole)
  - Clear in (ships check in port)
    - (shallow draft vessel) April 7 – 14, 2017
    - (main lay vessel) July 19 – Aug 15, 2017
  - Operational Period
    - (shallow draft vessel) April 7 – 14, 2017
    - (main lay vessel) July 19 – Aug 10, 2017



Transoceanic Subsea Fiber Cables

MAREA

Virginia Beach to Bilbao, Spain



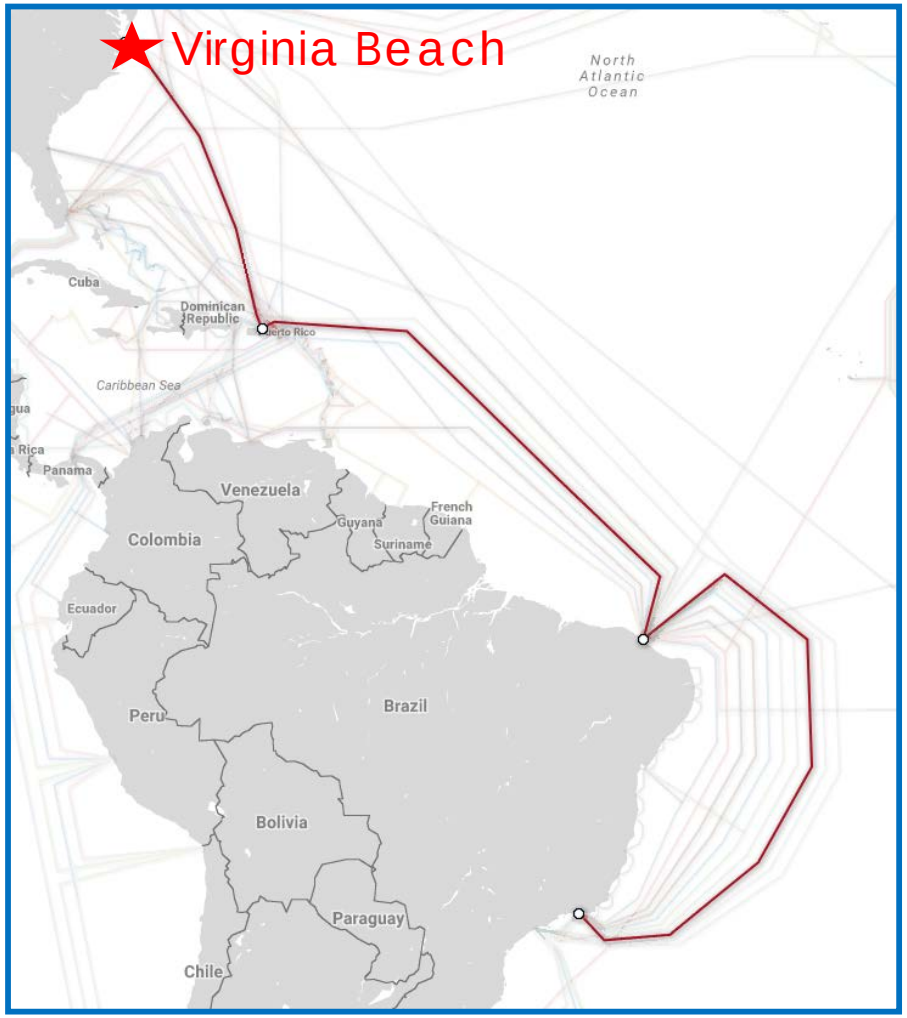
- Led by **Microsoft and Facebook, MAREA will be the highest-capacity subsea cable to ever cross the Atlantic**
- The new **6,600 km submarine cable system** will connect **Virginia Beach, Virginia to Bilbao, Spain**
- This new southern **route will provide greater diversity of connections & enhanced reliability** for customers
- Optimal connectivity to data centers on the East Coast
- Highest capacity cable to ever cross the Atlantic Ocean at 160 Tb/s

System Testing: **October 2017**
System Operational: **November/December 2017**

Transoceanic Subsea Fiber Cables

BRUSA

Virginia Beach to San Juan, Puerto Rico and Rio de Janeiro Brazil

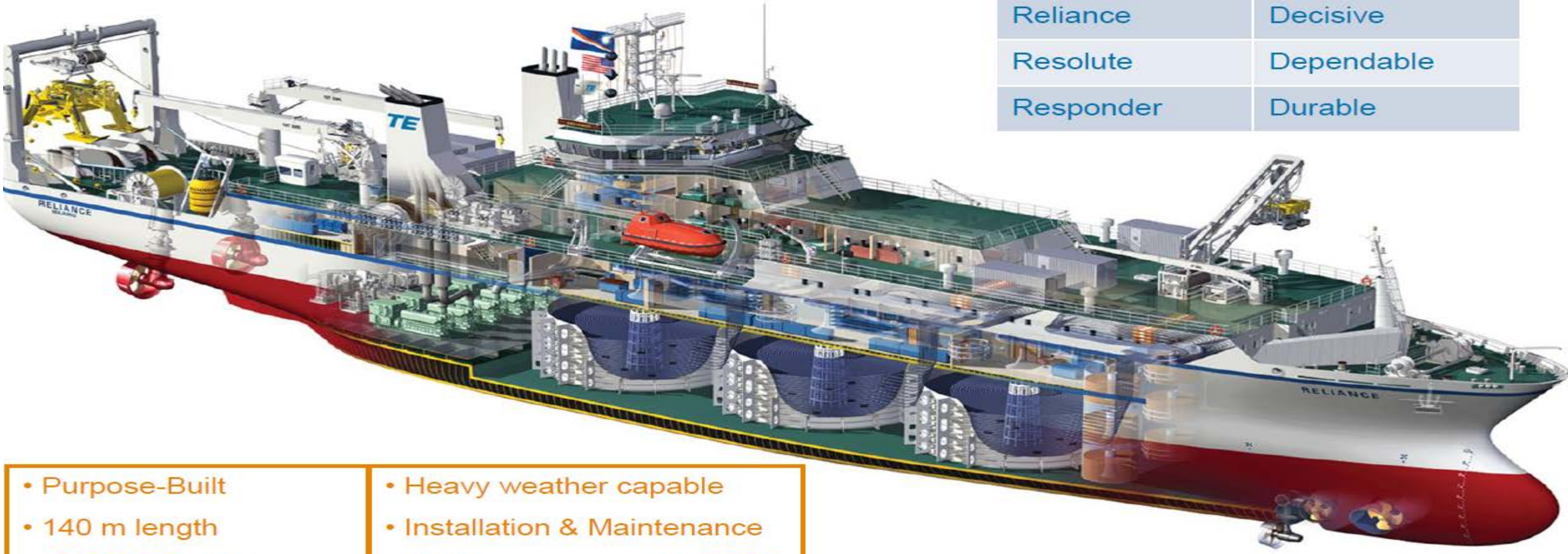


BRUSA Cable and Conduit Installation: **June 2018**
(dates per Telefonica)

- Led by Telxius Cable USA
- Nearly **11,000 km in length** linking **Rio de Janeiro** and **Fortaleza** (Brazil) with **San Juan** (Puerto Rico) and **Virginia Beach** (USA)
- Leading edge technology supporting **ultrafast transmission capacity**
- Increased end-to-end connectivity and the **availability of ultra high-speed broadband services**
- This new **infrastructure will address the exponential growth of data transmission** generated by its B2B customers, telecom operators, OTT players and end-consumers
- Will **improve communication reliability and deliver enhanced resilience by increasing the number of USA landing points**
- Will also provide the **lowest latency communication links between the two largest economies in the region, Brazil and USA**

Transoceanic Subsea Fiber Cables – Main Vessel

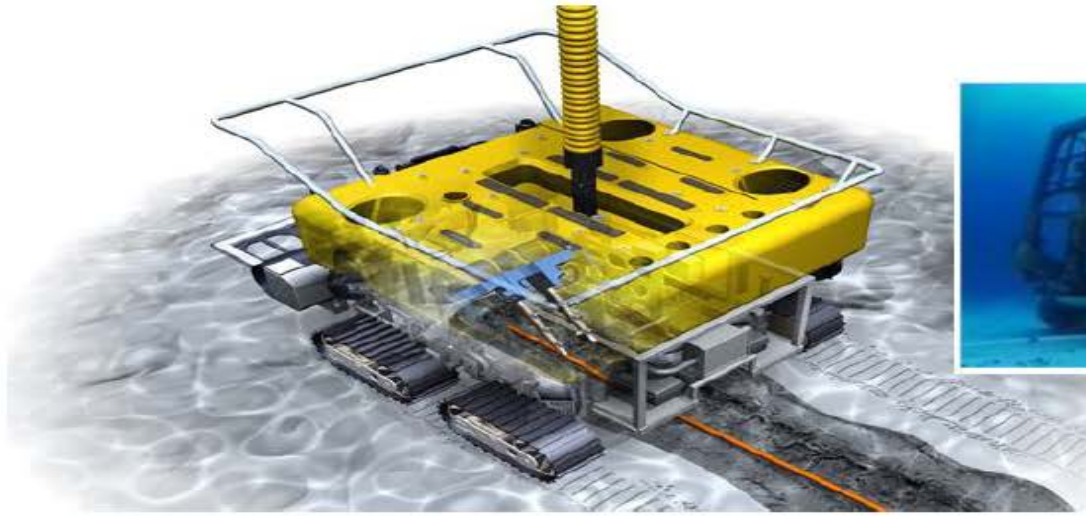
Reliance	Decisive
Resolute	Dependable
Responder	Durable



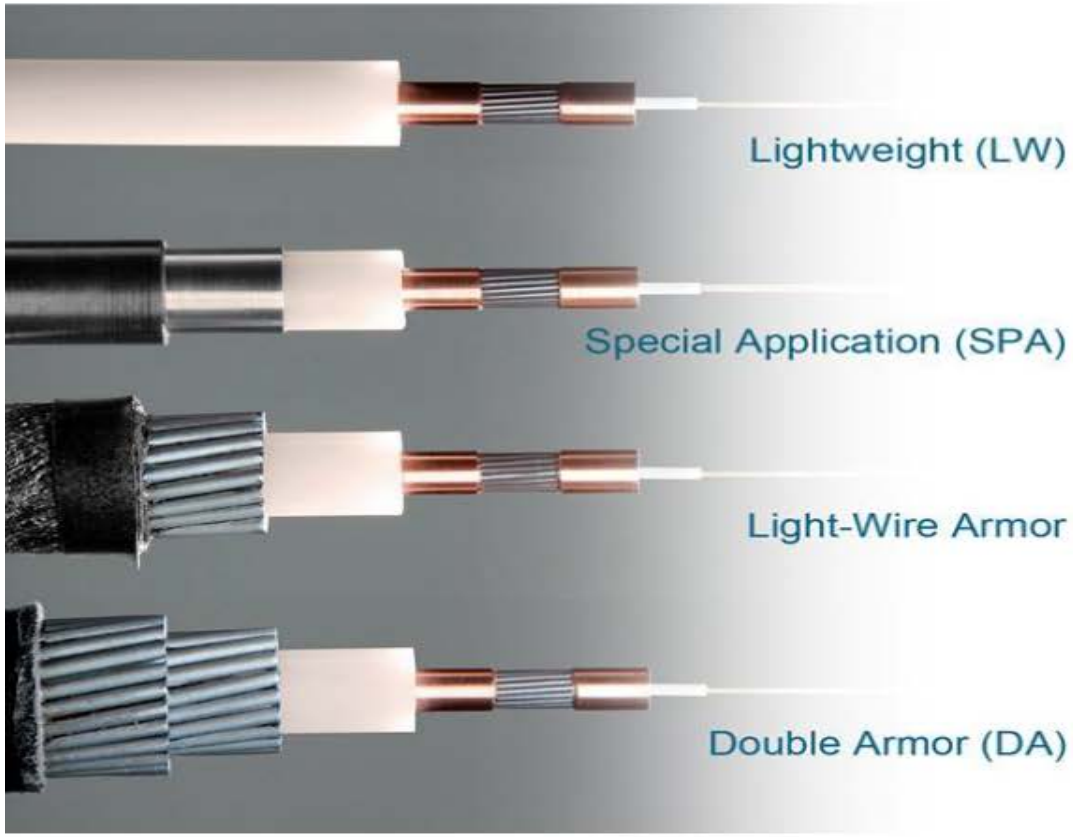
- Purpose-Built
- 140 m length
- 5,500 MT cable cap.
- 84 persons
- 60+ days endurance

- Heavy weather capable
- Installation & Maintenance
- Highly maneuverable (DP2)
- Plow & ROV equipped
- 60 MT A-Frame

Transoceanic Subsea Fiber Cables
Remotely Operated Vehicles (ROV)

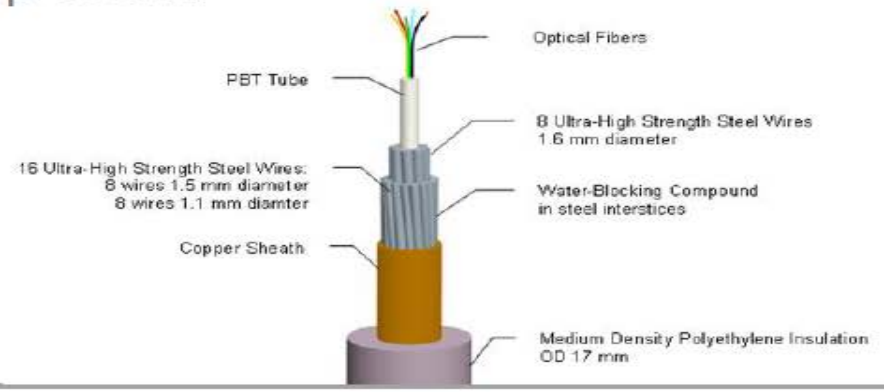


Transoceanic Subsea Fiber Cables

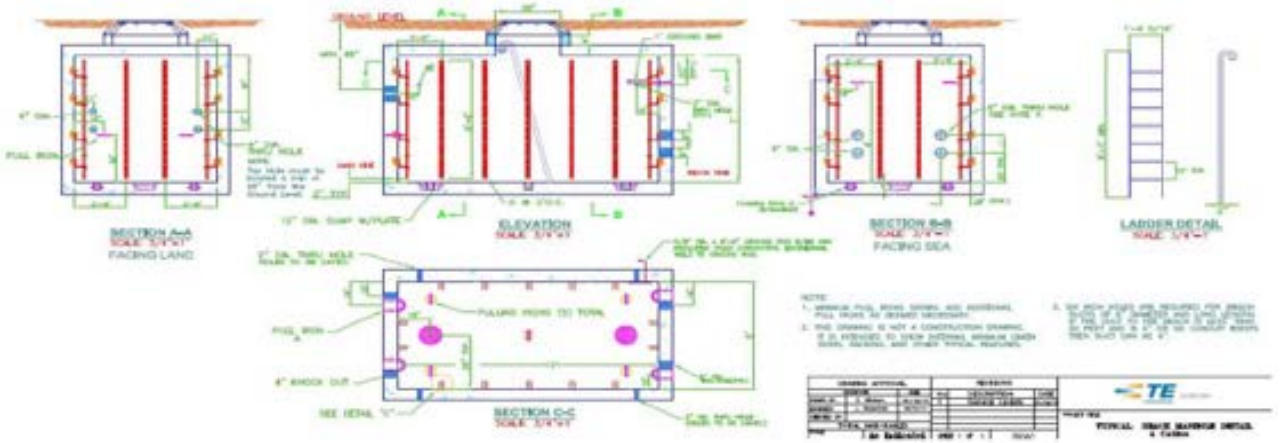


Undersea cables…

- protect optical fibers and an electrical conductor to carry telephone, internet & data communications traffic at ~2.5 TB/second;
- are built durable, yet flexible, to support system deployment, recovery, repair & re-deployment;
- are inert in the marine environment;
- offer various levels of protection from subsea conditions and external aggression, such as: rocky terrain, fishing activity, high risk of abrasion or crushing (e.g., anchoring), and the deep ocean.



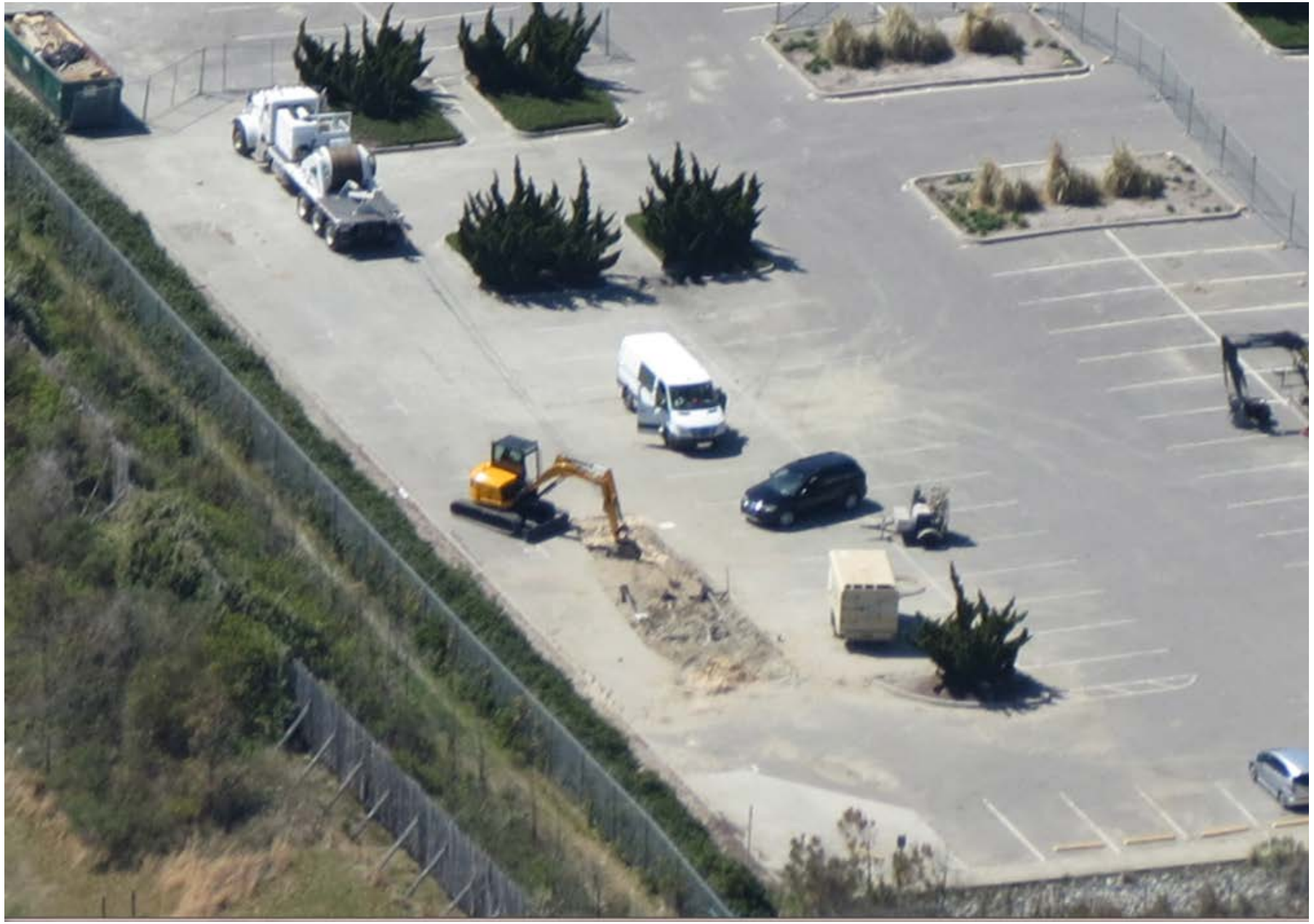
Transatlantic Subsea Fiber Cables



- **2 BMH's planned**
- **Typical BMH Design: 12' L x 6' W x 7' H**
- **Buried (below ground level) within the parking lot, with corresponding buried ocean ground bed anodes**
- **No Significant impact to the long-term functionality of the parking lot**

Transoceanic Subsea Fiber Cables – Shallow Water Vessel

Transoceanic Subsea Fiber Cables – Landing Point, Camp Pendleton

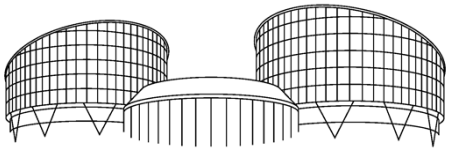


Transatlantic Subsea Fiber Cables

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix DD



EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

FIRST SECTION

CASE OF BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM

(Applications nos. 58170/13, 62322/14 and 24960/15)

JUDGMENT

STRASBOURG

13 September 2018

Request for referral to the Grand Chamber pending

This judgment will become final in the circumstances set out in Article 44 § 2 of the Convention. It may be subject to editorial revision.

TABLE OF CONTENTS

In the case of Big Brother Watch and Others v. the United Kingdom,

The European Court of Human Rights (First Section), sitting as a Chamber composed of:

Linos-Alexandre Sicilianos, *President,*
Kristina Pardalos,
Aleš Pejchal,
Ksenija Turković,
Armen Harutyunyan,
Pauliine Koskelo,
Tim Eicke, *judges,*
and Abel Campos, *Section Registrar,*

Having deliberated in private on 7 November 2017 and 3 July 2018,

Delivers the following judgment, which was adopted on the last-mentioned date:

PROCEDURE

1. The case originated in three applications (nos. 58170/13, 62322/14 and 24960/15) against the United Kingdom of Great Britain and Northern Ireland lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by the companies, charities, organisations and individuals listed in the Appendix ("the applicants") on 4 September 2013, 11 September 2014 and 20 May 2015 respectively.

2. The applicants were represented by Mr D. Carey, of Deighton Pierce Glynn Solicitors; Ms R. Curling of Leigh Day and Co. Solicitors; and Ms E. Norton of Liberty. The Government of the United Kingdom ("the Government") were represented by their Agent, Ms R. Sagoo of the Foreign and Commonwealth Office.

3. The applicants complained about the scope and magnitude of the electronic surveillance programmes operated by the Government of the United Kingdom.

4. The applications were communicated to the Government on 7 January 2014, 5 January 2015 and 24 November 2015. In the first case, leave to intervene was granted to Human Rights Watch, Access Now, Bureau Brandeis, Center For Democracy & Technology, European Network of National Human Rights Institutions and the Equality and Human Rights Commission, the Helsinki Foundation For Human Rights, the International Commission of Jurists, Open Society Justice Initiative, The Law Society of England and Wales and Project Moore; in the second case, to the Center For Democracy & Technology, the Helsinki Foundation For Human Rights, the International Commission of Jurists, the National Union of Journalists and

the Media Lawyers' Association; and in the third case, to Article 19, the Electronic Privacy Information Center and to the Equality and Human Rights Commission.

5. On 4 July 2017 the Chamber of the First Section decided to join the applications and hold an oral hearing. That hearing took place in public in the Human Rights Building, Strasbourg, on 7 November 2017.

There appeared before the Court:

(a) *for the Government*
Ms R. SAGOO, *Agent,*
Mr J. EADIE QC,
Mr J. MILFORD, *Counsel,*
Ms N. SAMUEL
Mr S. BOWDEN,
Mr M. ANSTEE,
Mr T. RUTHERFORD,
Ms L. MORGAN,
Mr B. NEWMAN, *Advisers.*

(b) for the applicants
Ms D. ROSE QC,
Ms H. MOUNTFIELD QC,
Mr M. RYDER QC, *Counsel,*
Mr R. MEHTA,
Mr C. MCCARTHY,
Mr D. CAREY,
Mr N. WILLIAMS *Advisers.*

6. The Court heard addresses by Mr Eadie, Ms Rose and Ms Mountfield, as well as their replies to questions put by the President and by Judges Koskelo, Harutyunyan, Eicke, Turković and Pardalos.

THE FACTS

I. THE CIRCUMSTANCES OF THE CASE

A. Background

7. The three applications were introduced following revelations by Edward Snowden relating to the electronic surveillance programmes

operated by the intelligence services of the United States of America and the United Kingdom.

8. The applicants, who are listed in the Appendix, all believed that due to the nature of their activities, their electronic communications were likely to have either been intercepted by the United Kingdom intelligence services; obtained by the United Kingdom intelligence services after being intercepted by foreign governments; and/or obtained by the United Kingdom authorities from Communications Service Providers ("CSPs").

B. The secret surveillance schemes

9. Internet communications are primarily carried over international sub-marine fibre optic cables operated by CSPs. Each cable may carry several "bearers", and there are approximately 100,000 of these bearers joining up the global Internet. A single communication over the Internet is divided into "packets" (units of data) which may be transmitted separately across multiple bearers. These packets will travel via a combination of the quickest and cheapest paths, which may also depend on the location of the servers. Consequently, some or all of the parts of any particular communication sent from one person to another, whether within the United Kingdom or across borders, may be routed through one or more other countries if that is the optimum path for the CSPs involved.

1. Government Communications Headquarters ("GCHQ")

10. The Edward Snowden revelations indicated that GCHQ (being one of the United Kingdom intelligence services) was running an operation, codenamed "TEMPORA", which allowed it to tap into and store huge volumes of data drawn from bearers.

11. According to the March 2015 Report of the Intelligence and Security Committee of Parliament ("the ISC report" – see paragraphs 151-159 below), GCHQ is operating two major processing systems for the bulk interception of communications. The United Kingdom authorities have neither confirmed nor denied the existence of an operation codenamed TEMPORA.

12. The first of the two processing systems referred to in the ISC report is targeted at a very small percentage of bearers. As communications flow across the targeted bearers, the system compares the traffic against a list of "simple selectors". These are specific identifiers (for example, an email address) relating to a known target. Any communications which match are collected; those that do not are automatically discarded. Analysts then carry out a "triage process" in relation to collected communications to determine which are of the highest intelligence value and should therefore be opened and read. In practice, only a very small proportion of the items collected

under this process are opened and read by analysts. GCHQ does not have the capacity to read all communications.

13. The second processing system is targeted at an even smaller number of bearers (a subset of those accessed by the process described in the paragraph above) which are deliberately targeted as those most likely to carry communications of intelligence interest. This second system has two stages: first, the initial application of a set of "processing rules" designed to discard material least likely to be of value; and secondly, the application of complex queries to the selected material in order to draw out those likely to be of the highest intelligence value. Those searches generate an index, and only items on that index may potentially be examined by analysts. All communications which are not on the list must be discarded.

14. The legal framework for bulk interception in force at the relevant time is set out in detail in the "Relevant Domestic law and practice" section below. In brief, section 8(4) of the Regulation of Investigatory Powers Act 2000 ("RIPA" – see paragraph 67 below) allows the Secretary of State to issue warrants for the "interception of external communications", and pursuant to section 16 of RIPA (see paragraphs 78-85 below) intercepted material cannot 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".

2. The United States' National Security Agency ("NSA")

15. The NSA has acknowledged the existence of two operations called PRISM and Upstream.

(a) PRISM

16. PRISM is a programme through which the United States' Government obtains intelligence material (such as communications) from Internet Service Providers ("ISPs"). Access under PRISM is specific and targeted (as opposed to a broad "data mining" capability). The United States' administration has stated that the programme is regulated under the Foreign Intelligence Service Act ("FISA"), and applications for access to material through PRISM have to be approved by the FISA Court, which is comprised of eleven senior judges.

17. Documents from the NSA leaked by Edward Snowden suggest that GCHQ has had access to PRISM since July 2010 and has used it to generate intelligence reports. GCHQ has acknowledged that it acquired information from the United States' which had been obtained via PRISM.

(b) Upstream

18. According to the leaked documents, the Upstream programme allows the collection of content and communications data from fibre-optic

cables and infrastructure owned by United States' CSPs. This programme has broad access to global data, in particular that of non-US citizens, which can then be collected, stored and searched using keywords.

C. Domestic proceedings in the first and second of the joined cases

19. The applicants in the first of the joined cases (application no. 58170/13) sent a pre-action protocol letter to the Government on 3 July 2013 setting out their complaints and seeking declarations that sections 1 and 3 of the Intelligence Services Act (see paragraphs 100-103 below), section 1 of the Security Services Act (see paragraph 99 below) and section 8 of RIPA (see paragraph 67 below) were incompatible with the Convention. In their reply of 26 July 2013, the Government stated that the effect of section 65(2) of RIPA was to exclude the jurisdiction of the High Court in respect of human rights complaints against the intelligence services. These complaints could however be raised in the Investigatory Powers Tribunal ("IPT"), a court established under RIPA to hear allegations by citizens of wrongful interference with their communications as a result of conduct covered by that Act, which was endowed with exclusive jurisdiction to investigate any complaint that a person's communications have been intercepted and, where interception has occurred, to examine the authority for such interception (see paragraphs 123-143 below). No further action was taken by these applicants.

20. The applicants in the second of the joined cases (application no. 62322/14) did not bring any domestic proceedings as they did not believe that they had an effective remedy for their Convention complaints.

D. Domestic proceedings in the third of the joined cases

21. The ten human rights organisations which are the applicants in the third of the joined cases (application no. 24960/15) each lodged a complaint before the IPT between June and December 2013. They alleged that the intelligence services, the Home Secretary and the Foreign Secretary had acted in violation of Articles 8, 10, and 14 of the Convention by: (i) accessing or otherwise receiving intercepted communications and communications data from the US Government under the PRISM and Upstream programmes ("the PRISM issue"); and (ii) intercepting, inspecting and retaining their communications and their communications data under the TEMPORA programme ("the section 8(4) issue"). The applicants sought disclosure of all relevant material relied on by the intelligence services in the context of their interception activities and, in particular, all policies and guidance.

22. On 14 February 2014 the IPT ordered that the ten cases be joined. It subsequently appointed Counsel to the Tribunal (see paragraph 142 below),

whose function is to assist the IPT in whatever way it directs, including by making representations on issues in relation to which not all parties can be represented (for example, for reasons of national security).

23. In their response to the applicants' claims, the Government adopted a "neither confirm nor deny" approach, that is to say, they declined to confirm or deny whether the applicants' communications had actually been intercepted. It was therefore agreed that the IPT would determine the legal issues on the basis of assumed facts to the effect that the NSA had obtained the applicants' communications and communications data via PRISM or Upstream and had passed them to GCHQ, where they had been retained, stored, analysed and shared; and that the applicants' communications and communications data had been intercepted by GCHQ under the TEMPORA programme and had been retained, stored, analysed and shared. The question was whether, on these assumed facts, the interception, retention, storage and sharing of data was compatible with Articles 8 and 10, taken alone and together with Article 14 of the Convention.

1. The hearing

24. The IPT, composed of two High Court Judges (including the President), a Circuit Judge and two senior barristers, held a five-day, public hearing from 14-18 July 2014. The Government requested an additional closed hearing in order to enable the IPT to consider GCHQ's unpublished – described during the public hearing as "below the waterline" – internal arrangements for processing data. The applicants objected, arguing that the holding of a closed hearing was not justified and that the failure to disclose the arrangements to them was unfair.

25. The request for a closed hearing was granted pursuant to Rule 9 of the IPT's Rules of Procedure (see paragraph 131 below) and on 10 September 2014 a closed hearing took place, at which neither the applicants nor their representatives were present. Instead, the IPT was "assisted by the full, perceptive and neutral participation ... of Counsel to the Tribunal", who performed the following roles: (i) identifying documents, parts of documents or gists that ought properly to be disclosed; (ii) making such submissions in favour of disclosure as were in the interests of the Claimants and open justice; and (iii) ensuring that all the relevant arguments (from the Claimants' perspective) on the facts and the law were put before the IPT.

26. In the closed hearing, the IPT examined the internal arrangements regulating the conduct and practice of the intelligence services. It found that it was entitled to look "below the waterline" to consider the adequacy of the applicable safeguards and whether any further information could or should be disclosed to the public in order to comply with the requirements of Articles 8 and 10.

27. On 9 October 2014 the IPT notified the applicants that it was of the view that there was some closed material which could be disclosed. It explained that it had invited the Government to disclose the material and that the Government had agreed to do so. The material was accordingly provided to the applicants in a note ("the 9 October disclosure") and the parties were invited to make submissions to the IPT on the disclosed material.

28. The applicants sought information on the context and source of the disclosure but the IPT declined to provide further details. The applicants made written submissions on the disclosure.

29. The respondents subsequently amended and amplified the disclosed material.

30. Following final disclosures made on 12 November 2014, the 9 October disclosure provided as follows:

> "The US Government has publicly acknowledged that the Prism system and Upstream programme ... permit the acquisition of communications to, from, or about specific tasked selectors associated with non-US persons who are reasonably believed to be located outside the United States in order to acquire foreign intelligence information. To the extent that the Intelligence Services are permitted by the US Government to make requests for material obtained under the Prism system (and/or ... pursuant to the Upstream programme), those requests may only be made for unanalysed intercepted communications (and associated communications data) acquired in this way.
>
> 1. 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. a relevant interception warrant under [RIPA] has already been issued by the Secretary of State, the assistance of the foreign government 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
>
> b. 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 contravene the principle established in *Padfield v. Minister of Agriculture, Fisheries and Food* [1968] AC 997 [that a public body is required to exercise its discretionary powers to promote (and not to circumvent) the policy and the objects of the legislation which created those powers] (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. In these circumstances, the question whether the request should be made would be considered and decided upon by the Secretary of State personally. Any such request would only be made in exceptional circumstances, and has not occurred as at the date of this statement.
>
> ...
>
> 2. Where the Intelligence Services receive intercepted communications content or communications data from the government of a country or territory outside the United

Kingdom, irrespective of whether it is/they are solicited or unsolicited, whether the content is analysed or unanalysed, or whether or not the communications data are associated with the content of communications, the communications content and data are, pursuant to internal 'arrangements', subject to the same internal rules and safeguards as the same categories of content or data, when they are obtained directly by the Intelligence Services as a result of interception under RIPA.

3. Those of the Intelligence Services that receive unanalysed intercepted material and related communications data from interception under a s.8(4) warrant have internal 'arrangements' that require a record to be created, explaining why access to the unanalysed intercepted material is required, before an authorised person is able to access such material pursuant to s.16 of RIPA.

4. The internal 'arrangements' of those of the Intelligence Services that receive unanalysed intercepted material and related communications data from interception under a s.8(4) warrant specify (or require to be determined, on a system-by-system basis) maximum retention periods for different categories of such data which reflect the nature and intrusiveness of the particular data at issue. The periods so specified (or determined) are normally no longer than 2 years, and in certain cases are significantly shorter (intelligence reports that draw on such data are treated as a separate category, and are retained for longer). Data may only be retained for longer than the applicable maximum retention period where prior authorisation has been obtained from a senior official within the particular Intelligence Service at issue on the basis that continued retention of the particular data at issue has been assessed to be necessary and proportionate (if the continued retention of any such data is thereafter assessed no longer to meet the tests of necessity and proportionality, such data are deleted). As far as possible, all retention periods are implemented by a process of automated deletion which is triggered once the applicable maximum retention period has been reached for the data at issue. The maximum retention periods are overseen by, and agreed with the Commissioner. As regards related communications data in particular, Sir Anthony May made a recommendation to those of the Intelligence Services that receive unanalysed intercepted material and related communications data from interception under a s8(4) warrant, and the interim Commissioner (Sir Paul Kennedy) has recently expressed himself to be content with the implementation of that recommendation.

5. The Intelligence Services' internal 'arrangements' under [the Security Services Act 1989], [the Intelligence Services Act 1994] and ss.15-16 of RIPA are periodically reviewed to ensure that they remain up-to-date and effective. Further, the Intelligence Services are henceforth content to consider, during the course of such periodic reviews, whether more of those internal arrangements might safely and usefully be put into the public domain (for example, by way of inclusion in a relevant statutory Code of Practice)."

2. The IPT's first judgment of 5 December 2014

31. The IPT issued its first judgment on 5 December 2014. The judgment addressed the arrangements then in place for intercepting and sharing data, making extensive reference throughout to this Court's case-law.

(a) The PRISM issue

32. The IPT accepted that the PRISM issue engaged Article 8 of the Convention, albeit at a "lower level" than the regime under consideration in

Weber and Saravia v. Germany (dec.), no. 54934/00, ECHR 2006‑XI. As a consequence, there would need to be compliance by the authorities involved in processing the data with the requirements of Article 8, particularly in relation to storage, sharing, retention and destruction. In the IPT's view, in order for the interference to be considered "in accordance with the law", there could not be unfettered discretion for executive action; rather, the nature of the rules had to be clear and the ambit of the rules had – in so far as possible – to be in the public domain (citing *Bykov v. Russia* [GC], no. 4378/02, §§ 76 and 78, 10 March 2009 and *Malone v. the United Kingdom*, 2 August 1984, Series A no. 82). However, it considered it plain that in the field of national security, much less was required to be put in the public domain and the degree of foreseeability required by Article 8 had to be reduced, otherwise the whole purpose of the steps taken to protect national security would be at risk (citing *Leander v. Sweden*, 26 March 1987, § 51, Series A no. 116).

33. The IPT continued:

> "41. We consider that what is required is a sufficient signposting of the rules or arrangements insofar as they are not disclosed ... We are satisfied that in the field of intelligence sharing it is not to be expected that rules need to be contained in statute (*Weber*) or even in a code (as was required by virtue of the Court's conclusion in *Liberty v. [the United Kingdom*, no. 58243/00, 1 July 2008]). It is in our judgment sufficient that:
>
> i) Appropriate rules or arrangements exist and are publicly known and confirmed to exist, with their content sufficiently signposted, such as to give an adequate indication of it (as per *Malone* ...).
>
> ii) They are subject to proper oversight."

34. The IPT noted that arrangements for information sharing were provided for in the statutory framework set out in the Security Services Act 1994 ("the SSA" – see paragraphs 98-99 below) and the Intelligence Services Act 1994 ("the ISA" – see paragraphs 100-103 below). It further referred to a witness statement of Charles Farr, the Director-General of the Office for Security and Counter Terrorism ("OSCT") at the Home Office, in which he explained that the statutory framework set out in those Acts was underpinned by detailed internal guidance, including arrangements for securing that the services only obtained the information necessary for the proper discharge of their functions. He further indicated that staff received mandatory training on the legal and policy framework in which they operated, including clear instructions on the need for strict adherence to the law and internal guidance. Finally, he stated that the full details of the arrangements were confidential since they could not be published safely without undermining the interests of national security.

35. The IPT therefore acknowledged that as the arrangements were not made known to the public, even in summary form, they were not accessible. However, the IPT considered it significant that the arrangements were

subject to oversight and investigation by the Intelligence and Security Committee of Parliament and the independent Interception of Communications Commissioner. Furthermore, it itself was in a position to provide oversight, having access to all secret information, and being able to adjourn into closed hearing to assess whether the arrangements referred to by Mr Farr existed and were capable of giving the individual protection against arbitrary interference.

36. In so far as the claimants challenged the IPT's decision to look "below the waterline" when assessing the adequacy of the safeguards, the IPT considered itself entitled to look at the internal arrangements in order to be satisfied that there were adequate safeguards and that what was described as "above the waterline" was accurate and gave a sufficiently clear signposting as to what was "below the waterline" without disclosing the detail of it. In this regard, the IPT did not accept that the holding of a closed hearing, as had been carried out in the applicants' case, was unfair. It accorded with the statutory procedure, gave the fullest and most transparent opportunity for hearing full arguments *inter partes* on hypothetical and actual facts with as much as possible heard in public, and protected the public interest and national security.

37. Having considered the arrangements "below the waterline", the IPT was satisfied that the 9 October disclosure (as subsequently amended) provided a clear and accurate summary of that part of the evidence given in the closed hearing which could and should be disclosed and that the rest of the evidence given in closed hearing was too sensitive for disclosure without risk to national security or to the "neither confirm nor deny" principle. It was further satisfied that it was clear that the preconditions for requesting information from the United States Government were either the existence of a section 8(1) warrant, or the existence of a section 8(4) warrant within whose ambit the proposed target's communications fell, together, if the individual was known to be in the British Islands, with a section 16(3) modification (see paragraph 80 below). In other words, any request pursuant to PRISM or Upstream in respect of intercept or communications data would be subject to the RIPA regime, unless it fell within the wholly exceptional scenario outlined in 1(b) of the material disclosed after the first hearing. However, a 1(b) request had never occurred.

38. The IPT nevertheless identified the following "matter of concern":

> "Although it is the case that any request for, or receipt of, intercept or communications data pursuant to Prism and/or Upstream is ordinarily subject to the same safeguards as in a case where intercept or communication data are obtained directly by the Respondents, if there were a 1(b) request, albeit that such request must go to the Secretary of State, and that any material so obtained must be dealt with pursuant to RIPA, there is the possibility that the s.16 protection might not apply. As already indicated, no 1(b) request has in fact ever occurred, and there has thus been no problem hitherto. We are however satisfied that there ought to be introduced a

procedure whereby any such request, if it be made, when referred to the Secretary of State, must address the issue of s.16(3)."

39. However, subject to this caveat, the IPT reached the following conclusions:

"(i) Having considered the arrangements below the waterline, as described in this 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.

(ii) This is of course of itself not sufficient, because the arrangements must be sufficiently accessible to the public. We are satisfied that they are sufficiently signposted by virtue of the statutory framework to which we have referred and the Statements of the ISC and the Commissioner quoted above, and as now, after the two closed hearings that we have held, publicly disclosed by the Respondents and recorded in this judgment.

(iii) These arrangements are subject to oversight.

(iv) The scope of the discretion conferred on the Respondents to receive and handle intercepted material and communications data and (subject to the s.8(4) issues referred to below) the manner of its exercise, are accordingly (and consistent with *Bykov* - see paragraph 37 above) accessible with sufficient clarity to give the individual adequate protection against arbitrary interference."

40. Finally, the IPT addressed an argument raised by Amnesty International only; namely, that the United Kingdom owed a positive obligation under Article 8 of the Convention to prevent or forestall the United States from intercepting communications including an obligation not to acquiesce in such interception by receiving its product. However, the IPT, citing *M. and Others v. Italy and Bulgaria*, no. 40020/03, § 127, 31 July 2012, noted that "the Convention organs have repeatedly stated that the Convention does not contain a right which requires a High Contracting Party to exercise diplomatic protection, or espouse an applicant's complaints under international law, or otherwise to intervene with the authorities of another state on his or her behalf". The IPT therefore rejected this submission.

(b) The section 8(4) issue

41. The IPT formulated four questions to be decided in order to determine whether the section 8(4) regime (which provided the legal framework for the bulk interception of external communications – see paragraph 67 below) was compatible with the Convention:

"(1) Is the difficulty of determining the difference between external and internal communications ... such as to cause the s.8(4) regime not to be in accordance with law contrary to Article 8(2)?

(2) Insofar as s.16 of RIPA is required as a safeguard in order to render the interference with Article 8 in accordance with law, is it a sufficient one?

(3) Is the regime, whether with or without s.16, sufficiently compliant with the *Weber* requirements, insofar as such is necessary in order to be in accordance with law?

(4) Is s. 16(2) indirectly discriminatory contrary to Article 14 of the Convention, and, if so, can it be justified?"

42. In relation to the first question, the applicants had contended that following the "sea-change in technology since 2000" substantially more communications were now external, and as a result the internal/external distinction in section 8(4) was no longer "fit for purpose". While the IPT accepted that the changes in technology had been substantial, and that it was impossible to differentiate at interception stage between external and internal communications, it found that the differences in view as to the precise definition of "external communications" did not *per se* render the section 8(4) regime incompatible with Article 8 § 2. In this regard, it considered that the difficulty in distinguishing between "internal" and "external" communications had existed since the enactment of RIPA and the changes in technology had not materially added to the quantity or proportion of communications which could or could not be differentiated as being external or internal at the time of interception. At worst, they had "accelerated the process of more things in the world on a true analysis being external than internal". In any case the distinction was only relevant at interception stage. The "heavy lifting" was done by section 16 of RIPA, which prevented intercepted material being 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" (see paragraphs 78-80 below). Furthermore, all communications intercepted under a section 8(4) warrant could only be considered for examination by reference to that section.

43. In respect of the second question, the IPT held that the section 16 safeguards, which applied only to intercept material and not to related communications data, were sufficient. Although it concluded that the *Weber* criteria also extended to communications data, it considered that there was adequate protection or safeguards by reference to section 15 (see paragraphs 72-77 below). In addition, insofar as section 16 offered greater protection for communications content than for communications data, the difference was justified and proportionate because communications data was necessary to identify individuals whose intercepted material was protected by section 16 (that is, individuals known to be in the British Islands).

44. Turning to the third question, the IPT concluded that the section 8(4) regime was sufficiently compliant with the *Weber* criteria and was in any event "in accordance with the law". With regard to the first and second requirements, it considered that the reference to "national security" was sufficiently clear (citing *Esbester v. the United Kingdom* (dec.),

no. 18601/91, 2 April 1993 and *Kennedy v. the United Kingdom*, no. 26839/05, 18 May 2010); the absence of targeting at the interception stage was acceptable and inevitable, as it had been in *Weber*; on their face, the provisions of paragraph 5.2 of the Interception of Communications Code of Practice, together with paragraphs 2.4, 2.5, 5.3, 5.4, 5.5 and 5.6 were satisfactory; there was no call for search words to be included in an application for a warrant or in the warrant itself, as this would unnecessarily undermine and limit the operation of the warrant and might in any event be entirely unrealistic; and there was no requirement for the warrant to be judicially authorised.

45. In considering the third, fourth, fifth and sixth of the *Weber* criteria, the IPT had regard to the safeguards in sections 15 and 16 of RIPA, the Interception of Communications Code of Practice, and the "below the waterline arrangements". It did not consider it necessary that the precise details of all the safeguards should be published or contained in either statute or code of practice. Particularly in the field of national security, undisclosed administrative arrangements, which by definition could be changed by the Executive without reference to Parliament, could be taken into account, provided that what is disclosed indicated the scope of the discretion and the manner of its exercise. This was particularly so when, as was the case here, the Code of Practice itself referred to the arrangements, and there was a system of oversight (being the Commissioner, the IPT itself, and the ISC) which ensured that these arrangements were kept under review. The IPT was satisfied that, as a result of what it had heard at the closed hearing and the 9 October disclosure as amended, there was no large databank of communications data being built up and that there were adequate arrangements in respect of the duration of the retention of data and its destruction. As with the PRISM issue, the IPT considered that the section 8(4) arrangements were sufficiently signposted in statute, in the Code of Practice, in the Interception of Communications Commissioner's reports and, now, in its own judgment.

46. As regards the fourth and final question, the IPT did not make any finding as to whether there was in fact indirect discrimination on grounds of national origin as a result of the different regimes applicable to individuals located in the British Islands and those located outside, since it considered that any indirect discrimination was sufficiently justified on the grounds that it was harder to investigate terrorist and criminal threats from abroad. Given that the purpose of accessing external communications was primarily to obtain information relating to those abroad, the consequence of eliminating the distinction would be the need to obtain a certificate under section 16(3) of RIPA (which exceptionally allowed access to material concerning persons within the British Islands intercepted under a section 8(4) warrant – see paragraph 80 below) in almost every case, which would radically undermine the efficacy of the section 8(4) regime.

47. Finally, in respect of Article 10, the applicants argued that its protection applied to investigatory NGOs as to journalists. Amnesty initially alleged before the IPT that there were likely to be no adequate arrangements for material protected by legal professional privilege, a complaint which was subsequently "hived off" to be dealt with in the *Belhadj* case (see paragraphs 92-94 below), to which Amnesty was joined as an additional claimant. No similar argument was made in respect of NGO confidence until 17 November 2014 (the first and second open hearings having taken place in July and October 2014). As the IPT considered that this argument could have been raised at any time, in its judgment it had been raised "far too late" to be incorporated into the ambit of the proceedings.

48. With regard to the remaining Article 10 complaints, the IPT noted that there was no separate argument over and above that arising in respect of Article 8. Although the IPT observed that there might be a special argument relating to the need for judicial pre-authorisation of a warrant (referring to *Sanoma Uitgevers B.V. v. the Netherlands* [GC], no. 38224/03, 14 September 2010), it emphasised that the applicants' case did not concern targeted surveillance of journalists or non-governmental organisations. In any case, in the context of untargeted monitoring via a section 8(4) warrant, it was "clearly impossible" to anticipate a judicial pre-authorisation prior to the warrant limited to what might turn out to impact upon Article 10. Although the IPT accepted that an issue might arise in the event that, in the course of examination of the contents, some question of journalistic confidence arose, it observed that there were additional safeguards in the Code of Practice in relation to treatment of such material.

49. Following the publication of the judgment, the parties were invited to make submissions on whether, prior to the disclosures made to the IPT, the legal regime in place in respect of the PRISM issue complied with Articles 8 and 10 and on the proportionality and lawfulness of any alleged interception of their communications. The IPT did not see any need for further submissions on the proportionality of the section 8(4) regime as a whole.

3. The IPT's second judgment of 6 February 2015

50. In its second judgment of 6 February 2015, the IPT considered whether, prior to its December 2014 judgment, the PRISM or Upstream arrangements breached Article 8 and/or 10 of the Convention.

51. It agreed that it was only by reference to the 9 October disclosure as amended that it was satisfied the current regime was "in accordance with the law". The IPT was of the view that without the disclosures made, there would not have been adequate signposting, as was required under Articles 8 and 10. It therefore made a declaration that prior to the disclosures made:

> "23. ... [T]he regime governing the soliciting, receiving, storing and transmitting by UK authorities of private communications of individuals located in the UK, which

have been obtained by US authorities pursuant to Prism and/or ... Upstream, contravened Articles 8 or 10 ECHR, but now complies."

4. The IPT's third judgment of 22 June 2015 as amended by its 1 July 2015 letter

52. The third judgment of the IPT, published on 22 June 2015, determined whether the applicants' communications obtained under PRISM or Upstream had been solicited, received, stored or transmitted by the United Kingdom authorities in contravention of Articles 8 and/or 10 of the Convention; and whether the applicants' communications had been intercepted, viewed, stored or transmitted by the United Kingdom authorities so as to amount to unlawful conduct or in contravention of Articles 8 and/or 10.

53. The IPT made no determination in favour of eight of the ten applicants. In line with its usual practice where it did not find in favour of the claimant, it did not confirm whether or not their communications had been intercepted. However, in relation to two applicants the IPT made determinations. The identity of one of the organisations was wrongly noted in the judgment and the error was corrected by the IPT's letter of 1 July 2015.

54. In respect of Amnesty International, the IPT found that email communications had been lawfully and proportionately intercepted and accessed pursuant to section 8(4) of RIPA but that the time-limit for retention permitted under the internal policies of GCHQ had been overlooked and the material had therefore been retained for longer than permitted. However, the IPT was satisfied that the material had not been accessed after the expiry of the relevant retention time-limit and that the breach could be characterised as a technical one. It amounted nonetheless to a breach of Article 8 and GCHQ was ordered to destroy any of the communications which had been retained for longer than the relevant period and to deliver one hard copy of the documents within seven days to the Interception of Communications Commissioner to retain for five years in case they were needed for any further legal proceedings. GCHQ was also ordered to provide a closed report within fourteen days confirming the destruction of the documents. No award of compensation was made.

55. In respect of the Legal Resources Centre, the IPT found that communications from an email address associated with the applicant had been intercepted and selected for examination under a section 8(4) warrant. Although it was satisfied the interception was lawful and proportionate and that selection for examination was proportionate, the IPT found that the internal procedure for selection was, in error, not followed. There had therefore been a breach of the Legal Resources Centre's Article 8 rights. However, the IPT was satisfied that no use was made of the material and that no record had been retained so the applicant had not suffered material

detriment, damage or prejudice. Its determination therefore constituted just satisfaction and no compensation was awarded.

II. RELEVANT DOMESTIC LAW AND PRACTICE

A. The interception of communications

1. Warrants: general

56. Section 1(1) of RIPA renders unlawful the interception of any communication in the course of its transmission by means of a public postal service or a public telecommunication system unless it takes place in accordance with a warrant under section 5 ("intercept warrant").

57. Section 5(2) allows the Secretary of State to authorise an intercept warrant if he believes: that it is necessary for the reasons set out in section 5(3), namely that it is in the interests of national security, for the purpose of preventing or detecting serious crime, or for safeguarding the economic well-being of the United Kingdom; and that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct. In assessing necessity and proportionality, account should be taken of whether the information sought under the warrant could reasonably be obtained by other means.

58. Section 81(2)(b) of RIPA defines "serious crime" as crime which satisfies one of the following criteria:

> "(a) that the offence or one of the offences that is or would be constituted by the conduct is an offence for which a person who has attained the age of twenty-one and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more;
>
> (b) that the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose."

59. Section 81(5) provides:

> "For the purposes of this Act detecting crime shall be taken to include–
>
> (a) establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed; and
>
> (b) the apprehension of the person by whom any crime was committed;
>
> and any reference in this Act to preventing or detecting serious crime shall be construed accordingly ..."

60. Section 6 provides that in respect of the intelligence services, only the Director General of MI5, the Chief of MI6 and the Director of GCHQ may apply for an intercept warrant.

61. There are two types of intercept warrant to which sections 5 and 6 apply: a targeted warrant as provided for by section 8(1); and an untargeted warrant as provided for by section 8(4).

62. By virtue of section 9 of RIPA, a warrant issued in the interests of national security or for safeguarding the economic well-being of the United Kingdom shall cease to have effect at the end of six months, and a warrant issued for the purpose of detecting serious crime shall cease to have effect after three months. At any time before the end of those periods, the Secretary of State may renew the warrant (for periods of six and three months respectively) if he believes that the warrant continues to be necessary on grounds falling within section 5(3). The Secretary of State shall cancel an interception warrant if he is satisfied that the warrant is no longer necessary on grounds falling within section 5(3).

63. Pursuant to section 5(6), the conduct authorised by an interception warrant shall be taken to include the interception of communications not identified by the warrant if necessary to do what is expressly authorised or required by the warrant; and the obtaining of related communications data.

64. Section 21(4) defines "communications data" as

> "(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, of 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."

65. The March 2015 Acquisition and Disclosure of Communications Data Code of Practice refers to these three categories as "traffic data", "service use information", and "subscriber information". Section 21(6) of RIPA further defines "traffic data" as data which identifies the person, apparatus, location or address to or from which a communication is transmitted, and information about a computer file or program accessed or run in the course of sending or receiving a communication.

66. Section 20 defines "related communications data", in relation to a communication intercepted in the course of its transmission by means of a postal service or telecommunication system, as communications data "obtained by, or in connection with, the interception"; and which "relates to the communication or to the sender or recipient, or intended recipient, of the communication".

2. Warrants: section 8(4)

(a) Authorisation

67. "Bulk interception" of communications is carried out pursuant to a section 8(4) warrant. Section 8(4) and (5) of RIPA allows the Secretary of State to issue a warrant for "the interception of external communications in the course of their transmission by means of a telecommunication system".

68. At the time of issuing a section 8(4) warrant, the Secretary of State must also issue a certificate setting out a description of the intercepted material which he considers it necessary to examine, and stating that he considers the examination of that material to be necessary for the reasons set out in section 5(3) (that is, that it is necessary in the interests of national security, for the purpose of preventing or detecting serious crime, or for safeguarding the economic well-being of the United Kingdom).

(b) "External" communications

69. Section 20 defines "external communication" as "a communication sent or received outside the British Islands".

70. In the course of the *Liberty* proceedings, Charles Farr, the Director General of the OSCT, indicated that two people in the United Kingdom who email each other are engaging in "internal communication" even if the email service was housed on a server in the United States of America; however, that communication may be intercepted as a "by-catch" of a warrant targeting external communications. On the other hand, a person in the United Kingdom who communicates with a search engine overseas is engaging in an external communication, as is a person in the United Kingdom who posts a public message (such as a tweet or Facebook status update), unless all the recipients of that message are in the British Islands.

71. Giving evidence to the Intelligence and Security Committee of Parliament in October 2014, the Secretary of State for the Foreign and Commonwealth considered that:

> "• In terms of an email, if one or both of the sender or recipient is overseas then this would be an external communication.
>
> • In terms of browsing the Internet, if an individual reads the Washington Post's website, then they have 'communicated' with a web server located overseas, and that is therefore an external communication.
>
> • In terms of social media, if an individual posts something on Facebook, because the web server is based overseas, this would be treated as an external communication.
>
> • In terms of cloud storage (for example, files uploaded to Dropbox), these would be treated as external communications, because they have been sent to a web server overseas."

3. Specific safeguards under RIPA

(a) Section 15

72. Pursuant to Section 15(1), it is the duty of the Secretary of State to ensure, in relation to all interception warrants, that such arrangements are in force as he considers necessary for securing that the requirements of subsections (2) and (3) are satisfied in relation to the intercepted material and any related communications data; and, in the case of warrants in relation to which there are section 8(4) certificates, that the requirements of section 16 are also satisfied.

73. Section 15(2) provides:

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

74. Section 15(3) provides:

> "The requirements of this subsection are satisfied in relation to the intercepted material and any related communications data if each copy made of any 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."

75. Pursuant to section 15(4), something is necessary for the authorised purposes if, and only if, it continues to be, or is likely to become, necessary as mentioned in section 5(3) of the Act (that is, it is necessary in the interests of national security, for the purpose of preventing or detecting serious crime; for the purpose of safeguarding the economic well-being of the United Kingdom; or for the purpose of giving effect to the provisions of any international mutual assistance agreement); it is necessary for facilitating the carrying out of any of the interception functions of the Secretary of State; it is necessary for facilitating the carrying out of any functions of the Interception of Communications Commissioner or of the IPT; it is necessary to ensure 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; or it is necessary for the performance of any duty imposed on any person under public records legislation.

76. Section 15(5) requires the arrangements in place to secure compliance with section 15(2) to include such arrangements as the Secretary

of State considers necessary for securing that every copy of the material or data that is made is stored, for so long as it is retained, in a secure manner.

77. Pursuant to section 15(6), the arrangements to which section 15(1) refers are not required to secure that the requirements of section 15(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. However, such arrangements are required to secure, in the case of every such warrant, that possession of the intercepted material and data and of copies of the material or data is surrendered to authorities of a country or territory outside the United Kingdom only if the requirements of section 15(7) are satisfied. Section 15(7) provides:

> "The requirements of this subsection are satisfied in the case of a warrant if it appears to the Secretary of State–
>
> (a) that requirements corresponding to those of subsections (2) and (3) will apply, to such extent (if any) as the Secretary of State thinks fit, in relation to any of the intercepted material or related communications data possession of which, or of any copy of which, is surrendered to the authorities in question; and
>
> (b) that restrictions are in force which would prevent, to such extent (if any) as the Secretary of State thinks fit, the doing of anything in, for the purposes of or in connection with any proceedings outside the United Kingdom which would result in such a disclosure as, by virtue of section 17, could not be made in the United Kingdom."

(b) Section 16

78. Section 16 sets out additional safeguards in relation to the interception of "external" communications under section 8(4) warrants. Section 16(1) requires that intercepted material may only be read, looked at or listened to by the persons to whom it becomes available by virtue of the warrant if and to the extent that it has been certified as material the examination of which is necessary as mentioned in section 5(3) of the Act; and falls within section 16(2). Section 20 defines "intercepted material" as the contents of any communications intercepted by an interception to which the warrant relates.

79. Section 16(2) provides:

> "Subject to subsections (3) and (4), 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."

80. Pursuant to section 16(3), intercepted material falls within section 16(2), notwithstanding that it is selected by reference to one of the factors mentioned in that subsection, if 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) of the Act; and the material relates only to communications sent during a period specified in the certificate that is no longer than the permitted maximum.

81. The "permitted maximum" is defined in section 16(3A) as follows:

> "(a) in the case of material the examination of which is certified for the purposes of section 8(4) as necessary in the interests of national security, six months; and
>
> (b) in any other case, three months."

82. Pursuant to section 16(4), intercepted material also falls within section 16(2), even if it is selected by reference to one of the factors mentioned in that subsection, if the person to whom the warrant is addressed believes, on reasonable grounds, that the circumstances are such that the material would fall within that subsection; or the conditions set out in section 16(5) are satisfied in relation to the selection of the material.

83. Section 16(5) provides:

> "Those conditions are satisfied in relation to the selection of intercepted material if –
>
> (a) it has appeared to the person to whom the warrant is addressed that there has been such a relevant change of circumstances as, but for subsection (4)(b), would prevent the intercepted material from falling within subsection (2);
>
> (b) since it first so appeared, a written authorisation to read, look at or listen to the material has been given by a senior official; and
>
> (c) the selection is made before the end of the permitted period."

84. Pursuant to section 16(5A), the "permitted period" means:

> "(a) in the case of material the examination of which is certified for the purposes of section 8(4) as necessary in the interests of national security, the period ending with the end of the fifth working day after it first appeared as mentioned in subsection (5)(a) to the person to whom the warrant is addressed; and
>
> (b) in any other case, the period ending with the end of the first working day after it first so appeared to that person."

85. Section 16(6) explains that a "relevant change of circumstances" means that it appears that either the individual in question has entered the British Islands; or that a belief by the person to whom the warrant is addressed in the individual's presence outside the British Islands was in fact mistaken.

86. Giving evidence to the Intelligence and Security Committee of Parliament in October 2014, the Secretary of State for the Foreign and Commonwealth explained that:

> "When an analyst selects communications that have been intercepted under the authority of an 8(4) warrant for examination, it does not matter what form of communication an individual uses, or whether his other communications are stored on a dedicated mail server or in cloud storage physically located in the UK, the US or anywhere else (and in practice the individual user of cloud services will not know where it is stored). If he or she is known to be in the British Islands it is not permissible to search for his or her communications by use of his or her name, e-mail address or any other personal identifier."

4. The Interception of Communications Code of Practice

87. Section 71 of RIPA provides for the adoption of codes of practice by the Secretary of State in relation to the exercise and performance of his powers and duties under the Act. Draft codes of practice must be laid before Parliament and are public documents. They can only enter into force in accordance with an order of the Secretary of State. The Secretary of State can only make such an order if a draft of the order has been laid before Parliament and approved by a resolution of each House.

88. Under section 72(1) of RIPA, a person exercising or performing any power or duty relating to interception of communications must have regard to the relevant provisions of a code of practice. The provisions of a code of practice may, in appropriate circumstances, be taken into account by courts and tribunals under section 72(4) RIPA.

89. The Interception of Communication Code of Practice ("the IC Code") was issued pursuant to section 71 of RIPA. The IC Code currently in force was issued in 2016.

90. Insofar as relevant, the IC Code provides:

> "3.2. There are a limited number of persons who can make an application for an interception warrant, or an application can be made on their behalf. These are:
>
> - The Director-General of the Security Service.
> - The Chief of the Secret Intelligence Service.
> - The Director of the Government Communications Headquarters (GCHQ).
> - The Director-General of the National Crime Agency (NCA handles interception on behalf of law enforcement bodies in England and Wales).
> - The Chief Constable of the Police Service of Scotland.
> - The Commissioner of the Police of the Metropolis (the Metropolitan Police Counter Terrorism Command handles interception on behalf of Counter Terrorism Units, Special Branches and some police force specialist units in England and Wales).
> - The Chief Constable of the Police Service of Northern Ireland.
> - The Commissioners of Her Majesty's Revenue & Customs (HMRC).
> - The Chief of Defence Intelligence.

- A person who, for the purposes of any international mutual assistance agreement, is the competent authority of a country or territory outside the UK.

3.3. Any application made on behalf of one of the above must be made by a person holding office under the Crown.

3.4. All interception warrants are issued by the Secretary of State. Even where the urgency procedure is followed, the Secretary of State personally authorises the warrant, although it is signed by a senior official.

Necessity and proportionality

3.5. Obtaining a warrant under RIPA will only ensure that the interception authorised is a justifiable interference with an individual's rights under Article 8 (right to respect for private and family life) of the European Convention on Human Rights (ECHR) if it is necessary and proportionate for the interception to take place. RIPA recognises this by first requiring that the Secretary of State believes that the authorisation is necessary for one or more of the following statutory grounds:

- In the interests of national security;
- To prevent or detect serious crime;
- To safeguard the economic well-being of the UK so far as those interests are also relevant to the interests of national security.

3.6. These purposes are set out in section 5(3) of RIPA. The Secretary of State must also believe that the interception is proportionate to what is sought to be achieved by that conduct. Any assessment of proportionality involves balancing the seriousness of the intrusion into the privacy or property of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative, operational or capability terms. The warrant will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that there is a potential threat to national security (for example) may not alone render the most intrusive actions proportionate. No interference should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

3.7. The following elements of proportionality should therefore 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;
- 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;
- 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.

...

Duration of interception warrants

3.18. Interception warrants issued on serious crime grounds are valid for an initial period of three months. Interception warrants issued on national security/economic well-being of the UK grounds are valid for an initial period of six months. A warrant issued under the urgency procedure (on any grounds) is valid for five working days following the date of issue unless renewed by the Secretary of State.

3.19. Upon renewal, warrants issued on serious crime grounds are valid for a further period of three months. Warrants renewed on national security/economic well-being of the UK grounds are valid for a further period of six months. These dates run from the date on the renewal instrument.

3.20. Where modifications to an interception warrant are made, the warrant expiry date remains unchanged. However, where the modification takes place under the urgency provisions, the modification instrument expires after five working days following the date of issue, unless it is renewed in line with the routine procedure.

3.21. Where a change in circumstance leads the intercepting agency to consider it no longer necessary, proportionate or practicable for a warrant to be in force, the agency must make a recommendation to the Secretary of State that it should be cancelled with immediate effect.

...

4. SPECIAL RULES ON INTERCEPTION WITH A WARRANT

Collateral intrusion

4.1. Consideration should be given to any interference with the privacy of individuals who are not the subject of the intended interception, especially where communications relating to religious, medical, journalistic or legally privileged material may be involved, or where communications between a Member of Parliament and another person on constituency business may be involved or communications between a Member of Parliament and a whistle-blower. An application for an interception warrant should state whether the interception is likely to give rise to a degree of collateral infringement of privacy. A person applying for an interception warrant must also consider measures, including the use of automated systems, to reduce the extent of collateral intrusion. Where it is possible to do so, the application should specify those measures. These circumstances and measures will be taken into account by the Secretary of State when considering a warrant application made under section 8(1) of RIPA. Should an interception operation reach the point where individuals other than the subject of the authorisation are identified as investigative targets in their own right, consideration should be given to applying for separate warrants covering those individuals.

Confidential information

4.2. 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.

4.3. 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. See also paragraphs 4.26 and 4.28 – 4.31 for additional safeguards that should be applied in respect of confidential journalistic material.

...

Communications involving confidential journalistic material, confidential personal information and communications between a Member of Parliament and another person on constituency business

4.26. Particular consideration must also be given to the interception of communications that involve confidential journalistic material, confidential personal information, or communications between a Member of Parliament and another person on constituency business. Confidential journalistic material is explained at paragraph 4.3. Confidential personal information is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and the material in question relates to his or her physical or mental health or to spiritual counselling. Such information can include both oral and written communications. Such information as described above is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence, or is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. For example, confidential personal information might include consultations between a health professional and a patient, or information from a patient's medical records.

...

4.28. Where the intention is to acquire confidential personal information, the reasons should be clearly documented and the specific necessity and proportionality of doing so should be carefully considered. If the acquisition of confidential personal information is likely but not intended, any possible mitigation steps should be considered and, if none is available, consideration should be given to whether special handling arrangements are required within the intercepting agency.

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.

4.32. The safeguards set out in paragraphs 4.28 – 4.31 also apply to any section 8(4) material (see chapter 6) which is selected for examination and which constitutes confidential information.

...

6. INTERCEPTION WARRANTS (SECTION 8(4))

6.1. This section applies to the interception of external communications by means of a warrant complying with section 8(4) of RIPA.

6.2. In contrast to section 8(1), a section 8(4) warrant instrument need not name or describe the interception subject or a set of premises in relation to which the interception is to take place. Neither does section 8(4) impose an express limit on the number of external communications which may be intercepted. For example, if the requirements of sections 8(4) and (5) are met, then the interception of all communications transmitted on a particular route or cable, or carried by a particular CSP, could, in principle, be lawfully authorised. This reflects the fact that section 8(4) interception is an intelligence gathering capability, whereas section 8(1) interception is primarily an investigative tool that is used once a particular subject for interception has been identified.

6.3. Responsibility for the issuing of interception warrants under section 8(4) of RIPA rests with the Secretary of State. When the Secretary of State issues a warrant of this kind, it must be accompanied by a certificate. The certificate ensures that a selection process is applied to the intercepted material so that only material described in the certificate is made available for human examination. If the intercepted material cannot be selected to be read, looked at or listened to with due regard to proportionality and the terms of the certificate, then it cannot be read, looked at or listened to by anyone.

Section 8(4) interception in practice

6.4. 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.

Definition of external communications

6.5. 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 the 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 external communication for the purposes of section 20 of RIPA, whether or not it is routed via IP addresses outside the British Islands, because the sender and intended recipient are within the British Islands.

Intercepting non-external communications under section 8(4) warrants

6.6. Section 5(6)(a) of RIPA makes clear that the conduct authorised by a section 8(4) warrant may, in principle, include the interception of communications which are not external communications to the extent this is necessary in order to intercept the external communications to which the warrant relates.

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 communications 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.

Application for a section 8(4) warrant

6.8. An application for a warrant is made to the Secretary of State. Interception warrants, when issued, are addressed to the person who submitted the application. The purpose of such a warrant will typically reflect one or more of the intelligence priorities set by the National Security Council (NSC).

6.9. Prior to submission, each application is subject to a review within the agency making the application. This involves scrutiny by more than one official, who will consider whether the application is for a purpose falling within section 5(3) of RIPA and whether the interception proposed is both necessary and proportionate.

6.10. Each application, a copy of which must be retained by the applicant, should contain the following information:

- Background to the operation in question:
  - Description of the communications to be intercepted, details of the CSP(s) and an assessment of the feasibility of the operation where this is relevant; and
  - Description of the conduct to be authorised, which must be restricted to the interception of external communications, or the conduct (including the interception of other communications not specifically identified by the warrant as foreseen under section 5(6)(a) of RIPA) it is necessary to undertake in order to carry out what is authorised or required by the warrant, and the obtaining of related communications data.
- The certificate that will regulate examination of intercepted material;
- An explanation of why the interception is considered to be necessary for one or more of the section 5(3) purposes;
- A consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct;
- Where an application is urgent, supporting justification;

- 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 sections 16(2)-16(6) of RIPA; and
- An assurance that all material intercepted will be handled in accordance with the safeguards required by sections 15 and 16 of RIPA (see paragraphs 7.2 and 7.10 respectively).

Authorisation of a section 8(4) warrant

6.11. Before issuing a warrant under section 8(4), the Secretary of State must believe the warrant is necessary:

- In the 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 UK so far as those interests are also relevant to the interests of national security.

6.12. The power to issue an interception warrant for the purpose of safeguarding the economic well-being of the UK (as provided for by section 5(3)(c) of RIPA), may only be exercised where it appears to the Secretary of State that the circumstances are relevant to the interests of national security. The Secretary of State will not issue a warrant on section 5(3)(c) grounds if a direct link between the economic well-being of the UK and national security is not established. Any application for a warrant on section 5(3)(c) grounds should therefore identify the circumstances that are relevant to the interests of national security.

6.13. The Secretary of State must also consider that the conduct authorised by the warrant is proportionate to what it seeks to achieve (section 5(2)(b)). In considering necessity and proportionality, the Secretary of State must take into account whether the information sought could reasonably be obtained by other means (section 5(4)).

6.14. When the Secretary of State issues a warrant of this kind, it must be accompanied by a certificate in which the Secretary of State certifies that he or she considers examination of the intercepted material to be necessary for one or more of the section 5(3) purposes. 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.

6.15. The Secretary of State has a duty to ensure that arrangements are in force for securing that only that material which has been certified as necessary for examination for a section 5(3) purpose, and which meets the conditions set out in section 16(2) to section 16(6) is, in fact, read, looked at or listened to. The Interception of Communications Commissioner is under a duty to review the adequacy of those arrangements.

Urgent authorisation of a section 8(4) warrant

6.16. RIPA makes provision (section 7(l)(b)) for cases in which an interception warrant is required urgently, yet the Secretary of State is not available to sign the

warrant. In these cases the Secretary of State will still personally authorise the interception but the warrant is signed by a senior official, following discussion of the case between officials and the Secretary of State. RIPA restricts the issue of warrants in this way to urgent cases where the Secretary of State has personally and expressly authorised the issue of the warrant (section 7(2)(a)), and requires the warrant to contain a statement to that effect (section 7(4)(a)).

6.17. A warrant issued under the urgency procedure lasts for five working days following the date of issue unless renewed by the Secretary of State, in which case it expires after three months in the case of serious crime or six months in the case of national security or economic well-being, in the same way as other section 8(4) warrants.

Format of a section 8(4) warrant

6.18. Each warrant is addressed to the person who submitted the application. A copy may then be served upon such providers of communications services as he or she believes will be able to assist in implementing the interception. CSPs will not normally receive a copy of the certificate. The warrant should include the following:

- A description of the communications to be intercepted;
- The warrant reference number; and
- Details of the persons who may subsequently modify the certificate applicable to the warrant in an urgent case (if authorised in accordance with section 10(7) of RIPA).

Modification of a section 8(4) warrant and/or certificate

6.19. Interception warrants and certificates may be modified under the provisions of section 10 of RIPA. A warrant may only be modified by the Secretary of State or, in an urgent case, by a senior official with the express authorisation of the Secretary of State. In these cases a statement of that fact must be endorsed on the modifying instrument, and the modification ceases to have effect after five working days following the date of issue unless it is endorsed by the Secretary of State.

6.20. A certificate must be modified by the Secretary of State, except in an urgent case where a certificate may be modified by a senior official provided that the official holds a position in which he or she is expressly authorised by provisions contained in the certificate to modify the certificate on the Secretary of State's behalf, or the Secretary of State has expressly authorised the modification and a statement of that fact is endorsed on the modifying instrument. In the latter case, the modification ceases to have effect after five working days following the date of issue unless it is endorsed by the Secretary of State.

6.21. Where the Secretary of State is satisfied that it is necessary, a certificate may be modified to authorise the selection of communications of an individual in the British Islands. An individual's location should be assessed using all available information. If it is not possible, to determine definitively where the individual is located using that information, an informed assessment should be made, in good faith, as to the individual's location. If an individual is strongly suspected to be in the UK, the arrangements set out in this paragraph will apply.

Renewal of a section 8(4) warrant

6.22. The Secretary of State may renew a warrant at any point before its expiry date. Applications for renewals are made to the Secretary of State and contain an

update of the matters outlined in paragraph 6.10 above. In particular, 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 purposes in section 5(3), and why it is considered that interception continues to be proportionate.

6.23. Where the Secretary of State is satisfied that the interception continues to meet the requirements of RIPA, the Secretary of State may renew the warrant. Where the warrant is issued on serious crime grounds, the renewed warrant is valid for a further three months. Where it is issued on national security/economic well-being grounds the renewed warrant is valid for six months. These dates run from the date of signature on the renewal instrument.

6.24. In those circumstances where the assistance of CSPs has been sought, a copy of the warrant renewal instrument will be forwarded to all those on whom a copy of the original warrant instrument has been served, providing they are still actively assisting. A renewal instrument will include the reference number of the warrant or warrants being renewed under this single instrument.

Warrant cancellation

6.25. The Secretary of State must cancel an interception warrant if, at any time before its expiry date, he or she is satisfied that the warrant is no longer necessary on grounds falling within section 5(3) of RIPA. Intercepting agencies will therefore need to keep their warrants under continuous review and must notify the Secretary of State if they assess that the interception is no longer necessary. In practice, the responsibility to cancel a warrant will be exercised by a senior official in the warrant issuing department on behalf of the Secretary of State.

6.26. The cancellation instrument will be addressed to the person to whom the warrant was issued (the intercepting agency). A copy of the cancellation instrument should be sent to those CSPs, if any, who have given effect to the warrant during the preceding twelve months.

Records

6.27. The oversight regime allows the Interception of Communications Commissioner to inspect the warrant application upon which the Secretary of State's decision is based, and the interception agency may be required to justify the content. Each intercepting agency should keep the following to be made available for scrutiny by the Commissioner as he or she may require:

- All applications made for warrants complying with section 8(4), and applications made for the renewal of such warrants;
- All warrants and certificates, and copies of renewal and modification instruments (if any);
- Where any application is refused, the grounds for refusal as given by the Secretary of State;
- The dates on which interception started and stopped.

6.28. Records should also be kept of the arrangements for securing that only material which has been certified for examination for a purpose under section 5(3) and which meets the conditions set out in section 16(2) – 16(6) of RIPA in accordance with section 15 of RIPA is, in fact, read, looked at or listened to. Records should be kept of the arrangements by which the requirements of section 15(2) (minimisation of

copying and distribution of intercepted material) and section 15(3) (destruction of intercepted material) are to be met. For further details see the chapter on "Safeguards".

7. SAFEGUARDS

7.1. All material intercepted under the authority of a warrant complying with section 8(1) or section 8(4) of RIPA and any related communications data must be handled in accordance with safeguards which the Secretary of State has approved in conformity with the duty imposed on him or her by RIPA. These safeguards are made available to the Interception of Communications Commissioner, and they must meet the requirements of section 15 of RIPA which are set out below. In addition, the safeguards in section 16 of RIPA apply to warrants complying with section 8(4). Any breach of these safeguards must be reported to the Interception of Communications Commissioner. The intercepting agencies must keep their internal safeguards under periodic review to ensure that they remain up-to-date and effective. During the course of such periodic reviews, the agencies must consider whether more of their internal arrangements might safely and usefully be put into the public domain.

The section 15 safeguards

7.2. Section 15 of RIPA requires that disclosure, copying and retention of intercepted material is limited to the minimum necessary for the authorised purposes. Section 15(4) of RIPA provides that something is necessary for the authorised purposes if the intercepted material:

- Continues to be, or is likely to become, necessary for any of the purposes set out in section 5(3) – namely, in the interests of national security, for the purpose of preventing or detecting serious crime, or for the purpose, in circumstances appearing to the Secretary of State to be relevant to the interests of national security, of safeguarding the economic well-being of the UK;
- Is necessary for facilitating the carrying out of the functions of the Secretary of State under Chapter I of Part I of RIPA;
- Is necessary for facilitating the carrying out of any functions of the Interception of Communications Commissioner or the Tribunal;
- Is necessary to ensure that a person conducting a criminal prosecution has the information needed to determine what is required of him or her by his or her duty to secure the fairness of the prosecution; or
- Is necessary for the performance of any duty imposed by the Public Record Acts.

Dissemination of intercepted material

7.3. The number of persons to whom any of the intercepted material is disclosed, and the extent of disclosure, is 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. It is enforced by prohibiting disclosure to persons who have not been appropriately vetted 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 or she needs to know about the intercepted material to carry out those duties. In the same way, only so much of the intercepted

material may be disclosed as the recipient needs. For example, if a summary of the intercepted 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 intercepted material is subsequently disclosed. In some cases this will be achieved by requiring the latter to obtain the originator's permission before disclosing the intercepted 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.

Copying

7.6. 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 intercepted material, but also extracts and summaries which identify themselves as the product of an interception, and any record referring to an interception which includes 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.

Storage

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 requirement to store intercept product securely applies to all those who are responsible for handling it, including CSPs. The details of what such a requirement will mean in practice for CSPs will be set out in the discussions they have with the Government before a Section 12 Notice is served (see paragraph 3.13).

Destruction

7.8. Intercepted material, and all copies, extracts and summaries which can be identified as the product of an interception, must be marked for deletion and securely destroyed as soon as possible once it is no longer needed for any of the authorised purposes. If such intercepted 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.

Personnel security

7.10. 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.

The section 16 safeguards

7.11. Section 16 provides for additional safeguards in relation to intercepted material gathered under section 8(4) warrants, requiring that the safeguards:

- Ensure that intercepted material is read, looked at or listened to by any person only to the extent that the intercepted material is certified; and
- Regulate the use of selection factors that refer to the communications of individuals known to be currently in the British Islands.

7.12. In addition, any individual selection of intercepted material must be proportionate in the particular circumstances (given section 6(1) of the Human Rights Act 1998).

7.13. The certificate ensures that a selection process is applied to material intercepted under section 8(4) warrants so that only material described in the certificate is made available for human examination (in the sense of being read, looked at or listened to). No official is permitted to gain access to the data other than as permitted by the certificate.

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 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.

7.20. The Secretary of State must ensure that the safeguards are in force before any interception under section 8(4) warrants can begin. The Interception of Communications Commissioner is under a duty to review the adequacy of the safeguards.

...

10. OVERSIGHT

10.1. RIPA provides for an Interception of Communications Commissioner, whose remit is to provide independent oversight of the use of the powers contained within the warranted interception regime under Chapter I of Part I of RIPA.

10.2. The Commissioner carries out biannual inspections of each of the nine interception agencies. The primary objectives of the inspections are to ensure that the Commissioner has the information he or she requires to carry out his or her functions under section 57 of RIPA and produce his or her report under section 58 of RIPA. This may include inspection or consideration of:

- The systems in place for the interception of communications;
- The relevant records kept by the intercepting agency;
- The lawfulness of the interception carried out; and
- Any errors and the systems designed to prevent such errors.

10.3. Any person who exercises the powers in RIPA Part I Chapter I must report to the Commissioner any action that is believed to be contrary to the provisions of RIPA or any inadequate discharge of section 15 safeguards. He or she must also comply with any request made by the Commissioner to provide any such information as the Commissioner requires for the purpose of enabling him or her to discharge his or her functions."

5. Statement of Charles Farr

91. In his witness statement prepared for the *Liberty* proceedings, Charles Farr indicated that, beyond the details set out in RIPA, the 2010 Code, and the draft 2016 Code (which had at that stage been published for consultation), the full details of the sections 15 and 16 safeguards were kept confidential. He had personally reviewed the arrangements and was satisfied that they could not safely be put in the public domain without undermining the effectiveness of the interception methods. However, the arrangements were made available to the Commissioner who is required by RIPA to keep them under review. Furthermore, each intercepting agency was required to keep a record of the arrangements in question and any breach must be reported to the Commissioner.

6. Belhadj and Others v. Security Service, Secret Intelligence Service, Government Communications Headquarters, the Secretary of State for the Home Department, and the Secretary of State for the Foreign and Commonwealth Office, IPT/13/132-9/H and IPT/14/86/CH

92. The applicants in this case complained of breaches of Articles 6, 8 and 14 of the Convention arising from the alleged interception of their legally privileged communications. Insofar as Amnesty International, in the course of the *Liberty* proceedings, complained about the adequacy of the arrangements for the protection of material protected by legal professional privilege ("LPP"), those complaints were "hived off" to be dealt with in this case, and Amnesty International was joined as a claimant (see paragraph 47 above).

93. In the course of the proceedings, the respondents conceded that by virtue of there not being in place a lawful system for dealing with LPP, from January 2010 the regime for the interception/obtaining, analysis, use,

disclosure and destruction of legally privileged material had not been in accordance with the law for the purposes of Article 8 § 2 of the Convention and was accordingly unlawful. The Security Service and GCHQ confirmed that they would work in the forthcoming weeks to review their policies and procedures in light of the draft Interception Code of Practice and otherwise.

94. The IPT subsequently held a closed hearing, with the assistance of Counsel to the Tribunal (see paragraph 142 below), to consider whether any documents or information relating to any legally privileged material had been intercepted or obtained by the respondents. In a determination of 29 March 2015 it found that only two documents containing material subject to legal professional privilege of any of the claimants had been held by the agencies, and they neither disclosed nor referred to legal advice. It therefore found that the claimant concerned had not suffered any detriment or damage, and that the determination provided adequate just satisfaction. It nevertheless required that GCHQ provide an undertaking that those parts of the documents containing legally privileged material would be destroyed or deleted; that a copy of the documents would be delivered to the Interception of Communications Commissioner to be retained for five years; and that a closed report would be provided within fourteen days confirming the destruction and deletion of the documents.

95. Draft amendments to both the Interception of Communications Code of Practice and the Acquisition of Communications Data Code of Practice were subsequently put out for consultation and the Codes which were adopted as a result contained expanded sections concerning access to privileged information.

B. Intelligence sharing

1. British-US Communication Intelligence Agreement

96. A British-US Communication Intelligence Agreement of 5 March 1946 governs the arrangements between the British and United States authorities in relation to the exchange of intelligence information relating to "foreign" communications, defined by reference to countries other than the United States, the United Kingdom and the Commonwealth. Pursuant to the agreement, the parties undertook to exchange the products of a number of interception operations relating to foreign communications.

2. Relevant statutory framework for the operation of the intelligence services

97. There are three intelligence services in the United Kingdom: the security service ("MI5"), the secret intelligence service ("MI6") and GCHQ.

(a) MI5

98. Pursuant to section 2 of the Security Services Act 1989 ("SSA"), it is the duty of the Director-General of MI5, who is appointed by the Secretary of State, to ensure that there are arrangements for securing that no information is obtained by MI5 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.

99. According to section 1 of the SSA, the functions of MI5 are 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; to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands; and to act in support of the activities of police forces, the National Crime Agency and other law enforcement agencies in the prevention and detection of serious crime.

(b) MI6

100. Section 2 of the Intelligence Services Act 1994 ("ISA") provides that the duties of the Chief of Service of MI6, who is appointed by the Secretary of State, include ensuring that there are arrangements for securing that no information is obtained by MI6 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, in the interests of national security, for the purposes of the prevention or detection of serious crime or for the purpose of any criminal proceedings.

101. According to section 1 of the ISA, the functions of MI6 are to obtain and provide information relating to the actions or intentions of persons outside the British Islands; and to perform other tasks relating to the actions or intentions of such persons. Those functions may only be exercised in the interests of national security, with particular reference to the State's defence and foreign policies; in the interests of the economic well-being of the United Kingdom; or in support of the prevention or detection of serious crime.

(c) GCHQ

102. Section 4 of the ISA provides that it is the duty of the Director of GCHQ, who is appointed by the Secretary of State, to ensure that there are arrangements for securing that it obtains no information 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.

103. According to section 3 of the ISA, one of the functions of GCHQ is 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. This function is exercisable only in the interests of national security, with particular reference to the State's defence and foreign policies; 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 in support of the prevention or detection of serious crime.

(d) Counter-Terrorism Act 2008

104. Section 19 of the Counter-Terrorism Act 2008 allows the disclosure of information to any of the intelligence services for the purpose of the exercise of any of their functions. Information obtained by an intelligence service in connection with the exercise of its functions may be used by that service in connection with the exercise of any of its other functions.

105. Information obtained by MI5 may be disclosed for the purpose of the proper discharge of its functions, for the purpose of the prevention or detection of serious crime, or for the purpose of any criminal proceedings. Information obtained by MI6 may be disclosed for the purpose of the proper discharge of its functions, in the interests of national security, for the purpose of the prevention or detection of serious crime, or for the purpose of any criminal proceedings. Information obtained by GCHQ may be disclosed by it for the purpose of the proper discharge of its functions or for the purpose of any criminal proceedings.

(e) The Data Protection Act 1998 ("DPA")

106. The DPA is the legislation transposing into United Kingdom law Directive 95/46/EC on the protection of personal data. Each of the intelligence services is a "data controller" for the purposes of the DPA and, as such, they are required to comply – subject to exemption by Ministerial certificate – with the data protection principles in Part 1 of Schedule 1, including:

> "(5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes ...

and

> "(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."

(f) The Official Secrets Act 1989 ("OSA")

107. A member of the intelligence services commits an offence under section 1(1) of the OSA if he discloses, without lawful authority, any

information, document or other article relating to security or intelligence which is in his possession by virtue of his position as a member of those services.

(g) The Human Rights Act 1998 ("HRA")

108. Pursuant to section 6 of the HRA, it is unlawful for a public authority to act in a way which is incompatible with a Convention right.

3. The Interception of Communications Code of Practice

109. Following the *Liberty* proceedings, the information contained in the 9 October disclosure was incorporated into the IC Code of Practice:

"12. RULES FOR REQUESTING AND HANDLING UNANALYSED INTERCEPTED COMMUNICATIONS FROM A FOREIGN GOVERNMENT

Application of this chapter

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

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

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

- A relevant interception warrant under RIPA has already been issued by the Secretary of State, the assistance of the foreign government is necessary to obtain the particular communications because they cannot be obtained under the relevant RIPA interception warrant and it is necessary and proportionate for the intercepting agency to obtain those communications; or
- Making the request for the particular communications 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 intercepting agency 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.

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 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.

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."

C. Acquisition of communications data

1. Chapter II of RIPA

110. Chapter II of Part 1 of RIPA sets out the framework under which public authorities may acquire communications data from CSPs.

111. Pursuant to section 22, authorisation for the acquisition of communications data from CSPs is granted by a "designated person", being a person holding such office, rank or position with relevant public authorities as are prescribed by an order made by the Secretary of State. The designated person may either grant authorisation for persons within the same "relevant public authority" as himself to "engage in conduct to which this Chapter applies" (authorisation under section 22(3)), or he may, by notice to the CSP, require it to either disclose data already in its possession, or to obtain and disclose data (notice under section 22(4)). For the purposes of section 22(3), "relevant public authorities" includes a police force, the National Crime Agency, Her Majesty's Revenue and Customs, any of the intelligence services, and any such public authority as may be specified by an order made by the Secretary of State.

112. Section 22(2) further provides that the designated person may only grant an authorisation under section 22(3) or give a notice under section 22(4) if he believes it is necessary for one of the following grounds:

"(a) in the interests of national security;

(b) for the purpose of preventing or detecting crime or of preventing disorder;

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

(d) in the interests of public safety;

(e) for the purpose of protecting public health;

(f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

(g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or

(h) for any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State."

113. He must also believe that obtaining the data is proportionate to what is sought to be achieved.

114. Section 23 requires that the authorisation or notice be granted in writing or, if not, in a manner which produces a record of it having been granted. It must also describe the conduct authorised, the communications data to be obtained or disclosed, set out the grounds on which it is believed necessary to grant the authorisation or give the notice, and specify the office, rank or position of the person giving the authorisation.

115. Authorisations under section 22(3) and notices under section 22(4) last for one month, but may be renewed at any time before the expiry of that period.

116. The person who has given a notice under section 22(4) may cancel it if he is satisfied that it is no longer necessary for one of the specified grounds, or it is no longer proportionate to what is sought to be achieved.

2. The Acquisition and Disclosure of Communications Data: Code of Practice

117. The Acquisition and Disclosure of Communications Data: Code of Practice, issued under section 71 RIPA and last updated in 2015, provides, as relevant:

"**1 INTRODUCTION**

1.1. This code of practice relates to the powers and duties conferred or imposed under Chapter II of Part I of the Regulation of Investigatory Powers Act 2000 ('RIPA'). It provides guidance on the procedures to be followed when acquisition of communications data takes place under those provisions. This version of the code replaces all previous versions of the code.

1.2. This code applies to relevant public authorities within the meaning of RIPA: those listed in section 25 or specified in orders made by the Secretary of State under section 25.

1.3. Relevant public authorities for the purposes of Chapter II of Part I of RIPA ('Chapter II') should not:

- use other statutory powers to obtain communications data from a postal or telecommunications operator unless that power provides explicitly for obtaining communications data, or is conferred by a warrant or order issued by the Secretary of State or a person holding judicial office; or
- require, or invite, any postal or telecommunications operator to disclose communications data by exercising any exemption to the principle of non-disclosure of communications data under the Data Protection Act 1998 ('the DPA').

...

1.7. The exercise of powers and duties under Chapter II is kept under review by the Interception of Communications Commissioner ('the Commissioner') appointed under section 57 of RIPA and by his inspectors who work from the Interception of Communications Commissioner's Office (IOCCO).

...

2 GENERAL EXTENT OF POWERS

Scope of Powers, Necessity and Proportionality

2.1. The acquisition of communications data under RIPA will be a justifiable interference with an individual's human rights under Articles 8 and, in certain circumstances, 10 of the European Convention on Human Rights only if the conduct being authorised or required to take place is both necessary and proportionate and in accordance with law.

2.2. RIPA stipulates that conduct to be authorised or required must be necessary for one or more of the purposes set out in section 22(2) of RIPA:

- in the interests of national security;
- for the purpose of preventing or detecting crime or of preventing disorder;
- in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security;
- in the interests of public safety;
- for the purpose of protecting public health;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
- for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health;
- to assist investigations into alleged miscarriages of justice;
- for the purpose of assisting in identifying any person who has died otherwise than as a result of crime or who is unable to identify himself because of a physical or mental condition, other than one resulting from crime (such as a natural disaster or an accident);

- in relation a person who has died or is unable to identify himself, for the purpose of obtaining information about the next of kin or other connected persons of such a person or about the reason for their death or condition; and
- for the purpose of exercising functions relating to the regulation of financial services and markets or to financial stability.

2.3. The purposes for which some public authorities may seek to acquire communications data are restricted by order. The designated person may only consider necessity on grounds open to their public authority and only in relation to matters that are the statutory or administrative function of their respective public authority. The purposes noted above should only be used by a public authority in relation to the specific (and often specialist) offences or conduct that it has been given the statutory function to investigate.

2.4. There is a further restriction upon the acquisition of communications data for the following purposes:

- in the interests of public safety;
- for the purpose of protecting public health; and
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department.

Only communications data within the meaning of section 21(4)(c) of RIPA [being subscriber information] may be acquired for these purposes and only by those public authorities permitted by order to acquire communications data for one or more of those purposes.

2.5. When a public authority wishes to acquire communications data, the designated person must believe that the acquisition, in the form of an authorisation or notice, is necessary. He or she must also believe that conduct to be proportionate to what is sought to be achieved by obtaining the specified communications data – that the conduct is no more than is required in the circumstances. This involves balancing the extent of the interference with an individual's rights and freedoms against a specific benefit to the investigation or operation being undertaken by a relevant public authority in the public interest.

2.6. As well as consideration of the rights of the individual under investigation, consideration must also be given to any actual or potential infringement of the privacy and other rights of individuals who are not the subject of the investigation or operation. An application for the acquisition of communications data should draw attention to any circumstances which give rise to significant collateral intrusion.

2.7. Particular consideration must also be given, when pertinent, to the right to freedom of expression.

2.8. Taking all these considerations into account in a particular case, an interference with the rights of an individual may still not be justified because the adverse impact on the rights of another individual or group of individuals is too severe.

2.9. Any conduct where the interference is excessive in relation to the aims of the investigation or operation, or is in any way arbitrary, will not be proportionate.

2.10. Before public authorities can request communications data, authorisation must be given by the designated person in the relevant authority. A designated person is someone holding a prescribed office, rank or position within a relevant public

authority that has been designated for the purpose of acquiring communications data by order.

2.11. The relevant public authorities for Chapter II are set out in section 25(1). They are:

- a police force (as defined in section 81(1) of RIPA);
- the National Crime Agency;
- HM Revenue and Customs;
- the Security Service;
- the Secret Intelligence Service; and
- the Government Communications Headquarters.

These and additional relevant public authorities are listed in the Regulation of Investigatory Powers (Communications Data) Order 201033 and any similar future orders made under section 25 of the Act.

Communications Data

2.12. The code covers any conduct relating to the exercise of powers and duties under Chapter II of Part I of RIPA to acquire or disclose communications data. Communications data is defined in section 21(4) of RIPA.

2.13. The term 'communications data' embraces the 'who', 'when', 'where', and 'how' of a communication but not the content, not what was said or written.

2.14. It includes the manner in which, and by what method, a person or machine communicates with another person or machine. It excludes what they say or what data they pass on within a communication including text, audio and video (with the exception of traffic data to establish another communication such as that created from the use of calling cards, redirection services, or in the commission of 'dial through' fraud and other crimes, where data is passed on to activate communications apparatus in order to obtain communications services fraudulently).

2.15. It can include the address on an envelope, the time and duration of a communication, the telephone number or email address of the originator and recipient, and sometimes the location of the device from which the communication was made. It can also include data relating to unsuccessful call attempts i.e. when the person being dialled does not answer the call, but where the network has been able to connect it successfully. It does not include data relating to an unconnected call i.e. when a call is placed, but the network is unable to carry it to its intended recipient. It covers electronic communications (not just voice telephony) and also includes postal services.

2.16. Communications data is generated, held or obtained in the provision, delivery and maintenance of communications services, those being postal services or telecommunications services. DRIPA clarified the definition of telecommunications service in section 2 of RIPA to make explicit that provision of access to systems for the creation, management or storage of communications is included in the provision of a service.

2.17. 'Communications service providers' may therefore include those persons who provide services where customers, guests or members of the public are provided with access to communications services that are ancillary to the provision of another service, for example in hotels, restaurants, libraries and airport lounges.

2.18. In circumstances where it is impractical for the data to be acquired from, or disclosed by, the service provider, or where there are security implications in doing so, the data may be sought from the CSP which provides the communications service offered by such hotels, restaurants, libraries and airport lounges. Equally, circumstances may necessitate the acquisition of further communications data for example, where a hotel is in possession of data identifying specific telephone calls originating from a particular guest room.

2.19. Consultation with the public authority's Single Point of Contact (SPoC) will determine the most appropriate plan for acquiring data where the provision of a communication service engages a number of providers, though it is the designated person who ultimately decides which of the CSPs should be given a notice. With the proliferation of modern communications media, including mobile telephony, internet communications, and social networks, and given that one individual can use many different forms of communications, the knowledge and experience of the SPoC in providing advice and guidance to the designated person is significant in ensuring appropriateness of any action taken to acquire the data necessary for an investigation. If a CSP, having been given a notice, believes that in future another CSP is better placed to respond, they should approach the authority to inform them of their view after disclosing the relevant data that they hold.

2.20. Any conduct to determine the CSP that holds, or may hold, specific communications data is not conduct to which the provisions of Chapter II apply. This includes, for example, establishing from information available to the public or, where necessary, from a service provider which provider makes available a specific service, such as a particular telephone number or an internet protocol address.

2.21. Communications data is defined as:

- traffic data (as defined by sections 21(4)(a) and 21(6) of RIPA) – this is data that is or has been comprised in or attached to a communication for the purpose of its transmission (see section starting at paragraph 2.24 of this code for further detail);
- service use information (as defined by section 21(4)(b) of RIPA) – this is the data relating to the use made by a person of a communications service (see section starting at paragraph 2.28 of this code for further detail); and
- subscriber information (as defined by section 21(4)(c) of RIPA) – this relates to information held or obtained by a CSP about persons to whom the CSP provides or has provided a communications services. Those persons will include people who are subscribers to a communications service without necessarily using that service and persons who use a communications service without necessarily subscribing to it (see section starting at paragraph 2.30 of this code for further detail).

2.22. The data available on individuals, and the level of intrusion, differs between the categories of data. The public authorities which can acquire the data and, in some cases, the level of seniority of the designated person differ according to the categories of data in question.

...

Traffic Data

2.24. RIPA defines certain communications data as 'traffic data' in sections 21(4)(a) and 21(6) of RIPA. This is data that is or has been comprised in or

attached to a communication for the purpose of transmitting the communication and which 'in relation to any communication':

- identifies, or appears to identify, any person, apparatus or location to or from which a communication is or may be transmitted;
- identifies or selects, or appears to identify or select, transmission apparatus;
- comprises signals that activate apparatus used, wholly or partially, for the transmission of any communication (such as data generated in the use of carrier pre-select or redirect communication services or data generated in the commission of, what is known as, 'dial through' fraud); or
- identifies data as data comprised in, or attached to, a communication. This includes data which is found at the beginning of each packet in a packet switched network that indicates which communications data attaches to which communication.

2.25. Traffic data includes data identifying a computer file or a computer program to which access has been obtained, or which has been run, by means of the communication – but only to the extent that the file or program is identified by reference to the apparatus in which the file or program is stored. In relation to internet communications, this means traffic data stops at the apparatus within which files or programs are stored, so that traffic data may identify a server or domain name (web site) but not a web page. For example, the fact that a subject of interest has visited pages at http://www.gov.uk/ can be acquired as communications traffic data (if available from the CSP), whereas that a specific webpage that was visited is http://www.gov.uk/government/collections/ripa--forms-2 may not be acquired as communications data (as it would be content).

2.26. Examples of traffic data, within the definition in section 21(6), include:

- information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);
- information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);
- information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
- routing information identifying apparatus through which a communication is or has been transmitted (for example, dynamic IP address allocation, file transfer logs and e mail headers – to the extent that content of a communication, such as the subject line of an e mail, is not disclosed);
- web browsing information to the extent that only a host machine, server, domain name or IP address is disclosed;
- anything, such as addresses or markings, written on the outside of a postal item (such as a letter, packet or parcel) that is in transmission and which shows the item's postal routing;
- records of correspondence checks comprising details of traffic data from postal items in transmission to a specific address; and

- online tracking of communications (including postal items and parcels).

...

Service Use Information

2.28. Data relating to the use made by any person of a postal or telecommunications service, or any part of it, is widely known as 'service use information' and falls within section 21(4)(b) of RIPA.

2.29. Service use information is, or can be, routinely made available by a CSP to the person who uses or subscribes to the service to show the use of a service or services and to account for service charges over a given period of time. Examples of data within the definition at section 21(4)(b) include:

- itemised telephone call records (numbers called);
- itemised records of connections to internet services;
- itemised timing and duration of service usage (calls and/or connections);
- information about amounts of data downloaded and/or uploaded;
- information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services;
- information about the use of forwarding/redirection services;
- information about selection of preferential numbers or discount calls; and
- records of postal items, such as records of registered post, recorded or special delivery postal items, records of parcel consignment, delivery and collection.

Subscriber Information

2.30. The third type of communications data, widely known as 'subscriber information', is set out in section 21(4)(c) of RIPA. This relates to information held or obtained by a CSP about persons to whom the CSP provides or has provided a communications service. Those persons will include people who are subscribers to a communications service without necessarily using that service and persons who use a communications service without necessarily subscribing to it.

2.31. Examples of data within the definition at section 21(4)(c) include:

- 'subscriber checks' (also known as 'reverse look ups') such as "who is the subscriber of phone number 01632 960 224?", "who is the account holder of e‑mail account example@example.co.uk?" or "who is entitled to post to web space www.example.co.uk?";
- information about the subscriber to a PO Box number or a Postage Paid Impression used on bulk mailings;
- information about the provision to a subscriber or accountholder of forwarding/redirection services, including delivery and forwarding addresses;
- subscribers' or account holders' account information, including names and addresses for installation, and billing including payment method(s), details of payments;

- information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services, and potentially static IP addresses;
- information about apparatus used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes; and
- information provided by a subscriber or account holder to a CSP, such as demographic information or sign‑up data (to the extent that information, such as a password, giving access to the content of any stored communications is not disclosed save where the requirement for such information is necessary in the interests of national security).

...

2.35. Additional types of data may fall into the category of subscriber information, as communications services have developed and broadened, for example where a CSP chooses to collect information about the devices used by their customers. Prior to the acquisition of data which does not fall into the illustrative list of traditional subscriber information above, specific consideration should be given to whether it is particularly sensitive or intrusive, in order to ensure that such a request is still necessary and proportionate, and compliant with Chapter II.

Further Guidance on Necessity and Proportionality

2.36. Training regarding necessity and proportionality should be made available to all those who participate in the acquisition and disclosure of communications data.

Necessity

2.37. In order to justify that an application is necessary, the application needs as a minimum to cover three main points:

- the event under investigation, such as a crime or vulnerable missing person;
- the person, such as a suspect, witness or missing person, and how they are linked to the event; and
- the communications data, such as a telephone number or IP address, and how this data is related to the person and the event.

2.38. Necessity should be a short explanation of the event, the person and the communications data and how these three link together. The application must establish the link between the three aspects to be able to demonstrate the acquisition of communications data is necessary for the statutory purpose specified.

Proportionality

2.39. Applications should include an outline of how obtaining the data will benefit the investigation or operation. If more than one item of data is being sought, the relevance of the additional data should be explained.

2.40. This should include explaining how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation. This justification should include confirmation that relevant less intrusive investigations have already been undertaken where possible. For example, the subscriber details of a

phone number may be obtainable from a phone book or other publically available sources.

2.41. The relevance of any time periods requested must be explained, outlining how these periods are proportionate to the event under investigation.

2.42. An examination of the proportionality of the application should particularly include a consideration of the rights (particularly to privacy and, in relevant cases, freedom of expression) of the individual and a balancing of these rights against the benefit to the investigation.

2.43. Collateral intrusion is the obtaining of any information relating to individuals other than the subject(s) of the investigation. Consideration of collateral intrusion forms part of the proportionality considerations, and becomes increasingly relevant when applying for traffic data or service use data. Applications should include details of what collateral intrusion may occur and how the time periods requested impact on the collateral intrusion. When there are no meaningful collateral intrusion risks, such as when applying for subscriber details of the person under investigation, the absence of collateral intrusion should be noted.

2.44. An examination of the proportionality of the application should also involve a consideration of possible unintended consequences and, when, relevant this should be noted. Unintended consequences of an application are outcomes that are not intended by the application.

2.45. Unintended consequences are more likely in more complicated requests for traffic data or in applications for the data of those in professions with duties of confidentiality. For example, if a journalist is a victim of crime, applications for service use data related to that journalist's phone number as part of the criminal investigation may also return some phone numbers of that journalist's sources, with unintended impact on freedom of expression. Such an application may still be necessary and proportionate but the risk of unintended consequences should be considered. The special considerations that arise in such cases are discussed further in the section on "Communications data involving certain professions".

3 GENERAL RULES ON THE GRANTING OF AUTHORISATIONS AND GIVING OF NOTICES

3.1. Acquisition of communications data under RIPA involves four roles within a relevant public authority:

- the applicant;
- the designated person;
- the single point of contact; and
- the senior responsible officer

3.2. RIPA provides two alternative means for acquiring communications data, by way of:

- an authorisation under section 22(3); or
- a notice under section 22(4).

An authorisation granted to a member of a public authority permits that person to engage in conduct relating to the acquisition and disclosure of communications data under Part I Chapter II of RIPA. A notice given to a postal or telecommunications operator requires it to disclose the relevant communications data held by it to a public

authority, or to obtain and disclose the data, when it is reasonably practicable for them to do so. Both authorisations and notices are explained in more detail within this chapter.

The applicant

3.3. The applicant is a person involved in conducting an investigation or operation for a relevant public authority who makes an application in writing or electronically for the acquisition of communications data. The applicant completes an application form, setting out for consideration by the designated person, the necessity and proportionality of a specific requirement for acquiring communications data.

3.4. An application may be made orally in exceptional circumstances, but a record of that application must be made in writing or electronically as soon as possible, and certainly within one working day (paragraphs 3.65 - 3.71 provide more detail on urgent procedures).

3.5. An application – the original or a copy of which must be retained by the SPoC within the public authority – must:

- include the name (or designation) and the office, rank or position held by the person making the application;
- include a unique reference number;
- include the operation name (if applicable) to which the application relates;
- specify the purpose for which the data is required, by reference to a statutory purpose under 22(2) of RIPA;
- describe the communications data required, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- describe whether the communications data relates to a victim, a witness, a complainant, a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;
- explain why the acquisition of that data is considered necessary and proportionate to what is sought to be achieved by acquiring it;
- consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the rights of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances;
- consider and, where appropriate, describe any possible unintended consequences of the application; and
- identify and explain the time scale within which the data is required.

3.6. The application should record subsequently whether it was approved by a designated person, by whom and when that decision was made. If approved, the application form should, to the extent necessary, be cross-referenced to any authorisation granted or notice given.

The designated person

3.7. The designated person is a person holding a prescribed office in a relevant public authority. It is the designated person's responsibility to consider the application and record their considerations at the time (or as soon as is reasonably practicable) in

writing or electronically. If the designated person believes the acquisition of communications data is necessary and proportionate in the specific circumstances, an authorisation is granted or a notice is given.

3.8. Individuals who undertake the role of a designated person must have current working knowledge of human rights principles and legislation, specifically those of necessity and proportionality, and how they apply to the acquisition of communications data under Chapter II and this code.

3.9. When considering proportionality, the designated person should apply particular consideration to unintended consequences. The seniority, experience and training of the designated person provides them with a particular opportunity to consider possible unintended consequences.

3.10. Designated persons must ensure that they grant authorisations or give notices only for purposes and only in respect of types of communications data that a designated person of their office, rank or position in the relevant public authority may grant or give.

3.11. The designated person shall assess the necessity for any conduct to acquire or obtain communications data taking account of any advice provided by the single point of contact (SPoC).

3.12. Designated persons must be independent from operations and investigations when granting authorisations or giving notices related to those operations.

3.13. Except where it is necessary to act urgently, in circumstances where a public authority is not able to call upon the services of a designated person who is independent from the investigation or operation, the Senior Responsible Officer must inform the Interception of Communications Commissioner of the circumstances and reasons (noting the relevant designated persons who, in these circumstances, will not be independent). These may include:

- small specialist criminal investigation departments within public authorities which are not law enforcement or intelligence agencies; and
- public authorities which have on-going operations or investigations immediately impacting on national security issues and are therefore not able to a call upon a designated person who is independent from their operations and investigations.

3.14. In all circumstances where public authorities use designated persons who are not independent from an operation or investigation this must be notified to the Commissioner at the next inspection. The details of the public authorities and the reasons such measures are being undertaken may be published and included in the Commissioner's report.

3.15. Where a designated person is not independent from the investigation or operation their involvement and their justification for undertaking the role of the designated person must be explicit in their recorded considerations.

3.16. Particular care must be taken by designated persons when considering any application to obtain communications data to identify apparatus (such as a mobile telephone) at or within a location or locations and at or between times on a given date or dates where the identity of the apparatus is unknown. Unless the application is based on information that the apparatus was used or was likely to have been used in a particular location or locations at a particular time or times it will, in practice, be rare

that any conduct to obtain communications data will be proportionate or the collateral intrusion justified.

...

The single point of contact

3.19. The single point of contact (SPoC) is an accredited individual trained to facilitate lawful acquisition of communications data and effective co-operation between a public authority and CSPs. Despite the name, in practice many organisations will have multiple SPoCs, working together. To become accredited an individual must complete a course of training appropriate for the role of a SPoC and have been issued the relevant SPoC authentication identifier. SPoCs in public authorities should be security cleared in accordance with their own organisation's requirements. Details of all accredited individuals are available to CSPs for authentication purposes.

3.20. Communications data should be treated as information with a classification of OFFICIAL and a caveat of SENSITIVE, though it may be classified higher if appropriate. When handling, processing, and distributing such information, SPoCs must comply with local security policies and operating procedures. The SENSITIVE caveat is for OFFICIAL information that is subject to 'need to know' controls so that only authorised personnel can have access to the material. This does not preclude, for example, the disclosure of material or the use of this material as evidence in open court when required. Rather, the classification and caveat of OFFICIAL - SENSITIVE makes clear that communications data must be treated with care, noting the impact on the rights to privacy and, where appropriate, freedom of expression of the subjects of interest and, depending on the data, possibly some of their communications contacts. Communications data acquired by public authorities must also by stored and handled in accordance with duties under the Data Protection Act.

3.21. An accredited SPoC promotes efficiency and good practice in ensuring only practical and lawful requirements for communications data are undertaken. This encourages the public authority to regulate itself. The SPoC provides objective judgement and advice to both the applicant and the designated person. In this way the SPoC provides a 'guardian and gatekeeper' function ensuring that public authorities act in an informed and lawful manner.

3.22. The SPoC should be in a position to:

- engage proactively with applicants to develop strategies to obtain communications data and use it effectively in support of operations or investigations;
- assess whether the acquisition of specific communications data from a CSP is reasonably practical or whether the specific data required is inextricably linked to other data;
- advise applicants on the most appropriate methodology for acquisition of data where the data sought engages a number of CSPs;
- advise applicants and designated persons on the interpretation of RIPA, particularly whether an authorisation or notice is appropriate;
- provide assurance to designated persons that authorisations and notices are lawful under RIPA and free from errors;

- consider and, where appropriate, provide advice to the designated person on possible unintended consequences of the application;
- provide assurance to CSPs that authorisations and notices are authentic and lawful;
- assess whether communications data disclosed by a CSP in response to a notice fulfils the requirement of the notice;
- assess whether communications data obtained by means of an authorisation fulfils the requirement of the authorisation; and
- assess any cost and resource implications to both the public authority and the CSP of data requirements.

3.23. The SPoC would normally be the person who takes receipt of any communications data acquired from a CSP (see paragraphs 3.33 and 3.49) and would normally be responsible for its dissemination to the applicant.

3.24. Public authorities unable to call upon the services of an accredited SPoC should not undertake the acquisition of communications data. Nonetheless, in the course of a joint investigation between authority A with no SPoC and authority B with RIPA communications data acquisition powers, authority B may, where necessary and proportionate, acquire communications data under RIPA to further the joint investigation.

3.25. In circumstances where a CSP is approached by a person who cannot be authenticated as an accredited individual and who seeks to obtain data under the provisions of RIPA, the CSP may refuse to comply with any apparent requirement for disclosure of data until confirmation of both the person's accreditation and their SPoC authentication identifier is obtained from the Home Office.

3.26. For each individual application, the roles of SPoC and designated persons will normally be carried out by two persons. In exceptional cases, such as those covered under the urgent oral procedure or, on rare occasions, for security reasons, both roles may be carried out by the same person. One person may, in separate applications, carry out the roles of either the SPoC or the designated person.

3.27. For each individual application, the roles of SPOC and Applicant will also normally be carried out by two persons. In exceptional cases, such as those covered under the urgent oral procedure or, on rare occasions, for security reasons, both roles may be carried out by the same person. One person may, in separate applications, carry out the roles of either the SPOC or the Applicant.

3.28. The same person must never be both the applicant and the designated person. Clearly, therefore, the same person should never be an applicant, a designated person and a SPoC.

3.29. Where a public authority seeks to obtain communications data using provisions providing explicitly for the obtaining of communications data (other than Chapter II of Part I of RIPA) or using statutory powers conferred by a warrant or order issued by the Secretary of State or a person holding judicial office, the SPoC should be engaged in the process of obtaining the data to ensure effective co-operation between the public authority and the CSP.

3.30. Occasionally public authorities will wish to request data from CSPs that is neither communications data nor the content of communications. Given the training

undertaken by a SPoC and the on-going nature of a SPoC's engagement with CSPs, it is good practice to engage the SPoC to liaise with the CSP on such requests.

The senior responsible officer

3.31. Within every relevant public authority a senior responsible officer must be responsible for:

- the integrity of the process in place within the public authority to acquire communications data;
- compliance with Chapter II of Part I of RIPA and with this code;
- oversight of the reporting of errors to IOCCO and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- engagement with the IOCCO inspectors when they conduct their inspections; and
- where necessary, oversight of the implementation of post-inspection action plans approved by the Commissioner.

Authorisations

3.32. An authorisation provides for persons within a public authority to engage in specific conduct, relating to a postal service or telecommunications system, to obtain communications data.

3.33. Any designated person in a public authority may only authorise persons working in the same public authority to engage in specific conduct, such as requesting the data via secure auditable communications data acquisition systems. This will normally be the public authority's SPoC, though local authorities must now use the National Anti-Fraud Network (see later in this chapter for more details).

3.34. The decision of a designated person whether to grant an authorisation shall be based upon information presented to them in an application.

3.35. An authorisation may be appropriate where:

- a CSP is not capable of obtaining or disclosing the communications data;
- there is an agreement in place between a public authority and a CSP relating to appropriate mechanisms for disclosure of communications data; or
- a designated person considers there is a requirement to identify a person to whom a service is provided but a CSP has yet to be conclusively determined as the holder of the communications data.

3.36. An authorisation is not served upon a CSP, although there may be circumstances where a CSP may require or may be given an assurance that conduct being, or to be, undertaken is lawful. That assurance may be given by disclosing details of the authorisation or the authorisation itself.

3.37. An authorisation – the original or a copy of which must be retained by the SPoC within the public authority – must:

- be granted in writing or, if not, in a manner that produces a record of it having been granted;

- describe the conduct which is authorised and describe the communications data to be acquired by that conduct specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- specify the purpose for which the conduct is authorised, by reference to a statutory purpose under section 22(2) of RIPA;
- specify the office, rank or position held by the designated person granting the authorisation. The designated person should also record their name (or designation) on any authorisation they grant; and
- record the date and, when appropriate to do so, the time when the authorisation was granted by the designated person.

...

3.40. At the time of giving a notice or granting an authorisation to obtain specific traffic data or service use data, a designated person may also authorise, to the extent necessary and proportionate at that time, the consequential acquisition of specific subscriber information relating to the traffic data or service use data to be obtained. This is relevant where there is a necessary and proportionate requirement to identify with whom a person has been in communication, for example:

- to identify with whom a victim was in contact, within a specified period, prior to their murder;
- to identify, where the target of an investigation or operation has been observed to make several calls from a public pay phone, the recipient of those calls;
- to identify a person making unlawful and unwarranted demands (as in the case of kidnap, extortion and blackmail demands and threats of violence); and
- where a victim or a witness has identified a specific communication or communications and corroboration of facts may reveal a potential offender or other witness.

3.41. At the time of giving a notice or granting an authorisation to obtain specific traffic data, a designated person may also authorise, to the extent necessary and proportionate at that time, the consequential acquisition of traffic data or service use information. This is relevant where there is a necessary and proportionate requirement to identify a person from the traffic data to be acquired, and the means to do so requires the CSP or another CSP to query their traffic data or service use information, for example:

- the CSP does not collect information about the customer within their customer information system but retains it in its original form as traffic data (such as a MAC or IMEI or an IP address); or
- where evidence or intelligence indicates there are several CSPs involved in routing a communication and there is a requirement to establish the recipient of the communication.

3.42. It is the duty of the senior responsible officer to ensure that the designated person, applicant or other person makes available to the SPoC such information as the senior responsible officer thinks necessary to ensure the integrity of any requirements for the acquisition of subscriber information to be obtained directly upon the

acquisition or disclosure of any traffic data or service use data, and their compliance with Chapter II and with this code.

Notices

3.43. The giving of a notice is appropriate where a CSP is able to retrieve or obtain specific data, and to disclose that data, unless the grant of an authorisation is more appropriate. A notice may require a CSP to obtain any communications data, if that data is not already in its possession.

3.44. The decision of a designated person whether to give a notice shall be based on information presented to them in an application.

3.45. The 'giving of a notice' means the point at which a designated person determines that a notice should be given to a CSP. In practice, once the designated person has determined that a notice should be given, it will be served upon a CSP in writing or, in an urgent situation, communicated to the CSP orally.

3.46. The notice should contain enough information to allow the CSP to comply with the requirements of the notice.

3.47. A notice – the original or a copy of which must be retained by the SPoC within the public authority – must:

- be given in writing or, if not, in a manner that produces a record, within the public authority, of its having been given;
- include a unique reference number and also identify the public authority;
- specify the purpose for which the notice has been given, by reference to a statutory purpose under 22(2) of RIPA;
- describe the communications data to be obtained or disclosed under the notice specifying, where relevant, any historic or future date(s)and, where appropriate, time period(s);
- include an explanation that compliance with the notice is a requirement of RIPA;
- specify the office, rank or position held by the designated person giving the notice. The name (or designation) of the designated person giving the notice should also be recorded;
- specify the manner in which the data should be disclosed. The notice should contain sufficient information including the contact details of the SPoC to enable a CSP to confirm the notice is authentic and lawful;
- record the date and, when appropriate to do so, the time when the notice was given by the designated person; and
- where appropriate, provide an indication of any urgency or time within which the CSP is requested to comply with the requirements of the notice.

3.48. A notice must not place a CSP under a duty to do anything which it is not reasonably practicable for the CSP to do. SPoCs should be mindful of the need to draft notices to ensure the description of the required data corresponds with the ways in which the CSP processes, retains and retrieves its data for lawful disclosure. CSPs cannot necessarily or reasonably edit or adapt their systems to take account of every possible variation of what may be specified in notices.

3.49. In giving notice a designated person may only require a CSP to disclose the communications data to the designated person or to a specified person working within the same public authority. This will normally be the public authority's SPoC.

3.50. Ordinarily the CSP should disclose, in writing or electronically, the communications data to which a notice relates not later than the end of the period of ten working days from the date the notice is served upon the CSP.

Duration of authorisations and notices

3.51. An authorisation or notice becomes valid on the date upon which authorisation is granted or notice given. It is then valid for a maximum of one month. This means the conduct authorised should have been commenced or the notice served within that month.

3.52. All authorisations and notices should refer to the acquisition or disclosure of data relating to a specific date(s) or period(s). Any period should be clearly indicated in the authorisation or notice. The start date and end date should be given, and where a precise start and end time are relevant these must be specified. Where the data to be acquired or disclosed is specified as 'current', the relevant date should be taken to be the date on which the authorisation was granted or the notice given by the designated person. There can be circumstances when the relevant date or period cannot be specified other than 'the last transaction' or 'the most recent use of the service'.

3.53. Where an authorisation or a notice relates to the acquisition or obtaining of specific data that will or may be generated in the future, the future period is restricted to no more than one month from the date upon which the authorisation was granted or the notice given.

3.54. Designated persons should specify the shortest possible period of time for any authorisation or notice. To do otherwise would impact on the proportionality of the authorisation or notice and impose an unnecessary burden upon the relevant CSP(s).

Renewal of authorisations and notices

3.55. Any valid authorisation or notice may be renewed for a period of up to one month by the grant of a further authorisation or the giving of a further notice. A renewed authorisation or notice takes effect upon the expiry of the authorisation or notice it is renewing.

3.56. Renewal may be appropriate where there is a continuing requirement to acquire or obtain data that will or may be generated in the future. The reasoning for seeking renewal should be set out by an applicant in an addendum to the application upon which the authorisation or notice being renewed was granted or given.

3.57. Where a designated person is granting a further authorisation or giving a further notice to renew an earlier authorisation or notice, the designated person should:

- have considered the reasons why it is necessary and proportionate to continue with the acquisition of the data being generated; and
- record the date and, when appropriate to do so, the time when the authorisation or notice is renewed.

Cancellation of notices and withdrawal of authorisations

3.58. A designated person who has given notice to a CSP under section 22(4) of RIPA shall cancel the notice if, at any time after giving the notice, it is no longer

necessary for the CSP to comply with the notice or the conduct required by the notice is no longer proportionate to what was sought to be achieved.

3.59. Reporting the cancellation of a notice to a CSP shall be undertaken by the designated person directly or, on that person's behalf, by the public authority's SPoC. Where human rights considerations are such that a notice should be cancelled with immediate effect the designated person or the SPoC will notify the CSP.

3.60. Cancellation of a notice reported to a CSP must:

- be undertaken in writing or, if not, in a manner that produces a record of the notice having been cancelled;
- identify, by reference to its unique reference number, the notice being cancelled; and
- record the date and, when appropriate to do so, the time when the notice was cancelled.

3.61. In cases where the SPoC has initiated the cancellation of a notice and reported the cancellation to the CSP, the designated person must confirm the decision in writing for the SPoC or, if not, in a manner that produces a record of the notice having been cancelled by the designated person. Where the designated person who gave the notice to the CSP is no longer available, this duty should fall on a person who has temporarily or permanently taken over the role of the designated person.

3.62. Similarly where a designated person considers an authorisation should cease to have effect, because the conduct authorised becomes unnecessary or no longer proportionate to what was sought to be achieved, the authorisation must be withdrawn. It may be the case that it is the SPoC or the applicant who is first aware that the authorisation is no longer necessary or proportionate. In such cases the SPoC (having been contacted by the applicant, where appropriate) may cease the authorised conduct, and then inform the designated person who granted the authorisation.

3.63. Withdrawal of an authorisation should:

- be undertaken in writing or, if not, in a manner that produces a record of it having been withdrawn;
- identify, by reference to its unique reference number, the authorisation being withdrawn;
- record the date and, when appropriate to do so, the time when the authorisation was cancelled; and
- record the name and the office, rank or position held by the designated person informed of the withdrawal of the authorisation.

3.64. When it is appropriate to do so, a CSP should be advised of the withdrawal of an authorisation, for example where details of an authorisation have been disclosed to a CSP.

Urgent oral giving of notice or grant of authorisation

3.65. In exceptionally urgent circumstances, an application for the giving of a notice or the grant of an authorisation may be made by an applicant, approved by a designated person and either notice given to a CSP or an authorisation granted orally. Circumstances in which an oral notice or authorisation may be appropriate include:

- an immediate threat of loss of human life, or for the protection of human life, such that a person's life might be endangered if the application procedure were undertaken in writing from the outset;
- an exceptionally urgent operational requirement where, within no more than 48 hours of the notice being given or the authorisation being granted orally, the acquisition of communications data will directly assist the prevention or detection of the commission of a serious crime and the making of arrests or the seizure of illicit material, and where that operational opportunity will be lost if the application procedure is undertaken in writing from the outset; or
- a credible and immediate threat to national security or a time-critical and unique opportunity to secure, or prevent the loss of, information of vital importance to national security where that threat might be realised, or that opportunity lost, if the application procedure were undertaken in writing from the outset.

3.66. The use of urgent oral process must be justified for each application within an investigation or operation. The fact that any part of an investigation or operation is undertaken urgently must not be taken to mean that all requirements to obtain communications data in connection with that investigation or operation be undertaken using the urgent oral process. It must be clear in each case why it was not possible, in the circumstances, to use the standard, written process.

...

3.69. Written notice must be given to the CSP retrospectively within one working day of the oral notice being given. Failure to do so will constitute an error which may be reported to the Commissioner by the CSP and must be recorded by the public authority (see the section on errors in Chapter 6, Keeping of Records, for more details).

3.70. After the period of urgency, a separate written process must be completed demonstrating the consideration given to the circumstances and the decisions taken. The applicant or the SPoC shall collate details or copies of control room or other operational logs which provide contemporaneous records of the consideration given to the acquisition of data, decision(s) made by the designated person and the actions taken in respect of the decision(s).

3.71. In all cases where urgent oral notice is given or authorisation granted, an explanation of why the urgent process was undertaken must be recorded.

Communications data involving certain professions

3.72. Communications data is not subject to any form of professional privilege – the fact a communication took place does not disclose what was discussed, considered or advised.

3.73. However the degree of interference with an individual's rights and freedoms may be higher where the communications data being sought relates to a person who is a member of a profession that handles privileged or otherwise confidential information (including medical doctors, lawyers, journalists, Members of Parliament, or ministers of religion). It may also be possible to infer an issue of sensitivity from the fact someone has regular contact with, for example, a lawyer or journalist.

3.74. Such situations do not preclude an application being made. However applicants, giving special consideration to necessity and proportionality, must draw

attention to any such circumstances that might lead to an unusual degree of intrusion or infringement of rights and freedoms, particularly regarding privacy and, where it might be engaged, freedom of expression. Particular care must be taken by designated persons when considering such applications, including additional consideration of whether there might be unintended consequences of such applications and whether the public interest is best served by the application.

3.75. Applicants must clearly note in all cases when an application is made for the communications data of those known to be in such professions, including medical doctors, lawyers, journalists, Members of Parliament, or ministers of religion. That such an application has been made must be recorded (see section 6 on keeping of records for more details), including recording the profession, and, at the next inspection, such applications should be flagged to the Interception of Communications Commissioner.

3.76. Issues surrounding the infringement of the right to freedom of expression may arise where a request is made for the communications data of a journalist. There is a strong public interest in protecting a free press and freedom of expression in a democratic society, including the willingness of sources to provide information to journalists anonymously. Where an application is intended to determine the source of journalistic information, there must therefore be an overriding requirement in the public interest, and the guidance at paragraphs 3.78–3.24 should be followed.

3.77. Where the application is for communications data of a journalist, but is not intended to determine the source of journalistic information (for example, where the journalist is a victim of crime or is suspected of committing a crime unrelated to their occupation), there is nevertheless a risk of collateral intrusion into legitimate journalistic sources. In such a case, particular care must therefore be taken to ensure that the application considers whether the intrusion is justified, giving proper consideration to the public interest. The necessity and proportionality assessment also needs to consider whether alternative evidence exists, or whether there are alternative means for obtaining the information being sought. The application should draw attention to these matters.

Applications to determine the source of journalistic information

3.78. In the specific case of an application for communications data, which is made in order to identify a journalist's source, and until such time as there is specific legislation to provide judicial authorisation for such applications, those law enforcement agencies, including the police, National Crime Agency and Her Majesty's Revenue and Customs, in England and Wales with powers under the Police and Criminal Evidence Act 1984 (PACE) must use the procedures of PACE to apply to a court for a production order to obtain this data. Relevant law enforcement agencies in Northern Ireland must apply for a production order under the PACE (Northern Ireland Order) 1989. Law enforcement agencies in Scotland must use the appropriate legislation or common law powers to ensure judicial authorisation for communications data applications to determine journalistic sources.

3.79. Communications data that may be considered to determine journalistic sources includes data relating to:

- journalists' communications addresses;
- the communications addresses of those persons suspected to be a source; and

- communications addresses of persons suspected to be acting as intermediaries between the journalist and the suspected source.

3.80. Each authority must keep a central record of all occasions when such an application has been made, including a record of the considerations.

3.81. This includes that, where the police suspect wrong‑doing that includes communications with a journalist, the application must consider properly whether that conduct is criminal and of a sufficiently serious nature for rights to freedom of expression to be interfered with where communications data is to be acquired for the purpose of identifying a journalist's source.

3.82. As described in paragraph 3.29 above, the SPoC should be engaged in this process, to ensure appropriate engagement with the CSPs.

3.83. If and only if there is a believed to be an immediate threat of loss of human life, such that a person's life might be endangered by the delay inherent in the process of judicial authorisation, law enforcement agencies may continue to use the existing internal authorisation process under RIPA. Such applications must be flagged to the Interception of Communications Commissioner as soon as reasonably practicable, as agreed with the Commissioner. If additional communications data is later sought as part of the same investigation, but where a threat to life no longer exists, judicial authorisation must be sought.

3.84. The requirement for judicial oversight does not apply where applications are made for the communications data of those known to be journalists but where the application is not to determine the source of journalistic information. This includes, for example, where the journalist is a victim of crime or is suspected of committing a crime unrelated to their occupation.

Local authority authorisation procedure

3.85. Local authorities must fulfil two additional requirements when acquiring communications data that differ from other public authorities. Firstly, the request must be made through a SPoC at the National Anti‑Fraud Network ('NAFN'). Secondly, the request must receive prior judicial approval.

...

6 KEEPING OF RECORDS

Records to be kept by a relevant public authority

6.1. Applications, authorisations, copies of notices, and records of the withdrawal of authorisations and the cancellation of notices, must be retained by the relevant public authority in written or electronic form, and physically attached or cross‑referenced where they are associated with each other. The public authority should also keep a record of the date and, when appropriate to do so, the time when each notice or authorisation is given or granted, renewed or cancelled. Records kept by the public authority must be held centrally by the SPoC or in accordance with arrangements previously agreed with the Commissioner.

6.2. These records must be available for inspection by the Commissioner and retained to allow the Investigatory Powers Tribunal, established under Part IV of RIPA, to carry out its functions.

6.3. Where the records contain, or relate to, material obtained directly as a consequence of the execution of an interception warrant, those records must be treated

in accordance with the safeguards which the Secretary of State has approved in accordance with section 15 of RIPA.

...

6.5. Each relevant public authority must also keep a record of the following information:

A. the number of applications submitted by an applicant to a SPoC requesting the acquisition of communications data (including orally);

B. the number of applications submitted by an applicant to a SPoC requesting the acquisition of communications data (including orally), which were referred back to the applicant for amendment or declined by the SPoC, including the reason for doing so;

C. the number of applications submitted to a designated person for a decision to obtain communications data (including orally), which were approved after due consideration;

D. the number of applications submitted to a designated person for a decision to obtain communications data (including orally), which were referred back to the applicant or rejected after due consideration, including the reason for doing so;

E. the number of notices requiring disclosure of communications data (not including urgent oral applications);

F. the number of authorisations for conduct to acquire communications data (not including urgent oral applications);

G. the number of times an urgent application is approved orally;

H. the number of times an urgent notice is given orally, or an urgent authorisation granted orally, requiring disclosure of communications data;

I. the priority grading of the application for communications data, as set out at paragraph 3.5 and footnote 52 of this code;

J. whether any part of the application relates to a person who is a member of a profession that handles privileged or otherwise confidential information (such as a medical doctor, lawyer, journalist, Member of Parliament, or minister of religion) (and if so, which profession); and

K. the number of items of communications data sought, for each notice given, or authorisation granted (including orally).

6.6. For each item of communications data included within a notice or authorisation, the relevant public authority must also keep a record of the following:

A. the Unique Reference Number (URN) allocated to the application, notice and/or authorisation;

B. the statutory purpose for which the item of communications data is being requested, as set out at section 22(2) of RIPA;

C. where the item of communications data is being requested for the purpose of preventing or detecting crime or of preventing disorder, as set out at section 22(2)(b) of RIPA, the crime type being investigated;

D. whether the item of communications data is traffic data, service use information, or subscriber information, as described at section 21 (4) of RIPA, and Chapter 2 of this code;

E. a description of the type of each item of communications data included in the notice or authorisation;

F. whether the item of communications data relates to a victim, a witness, a complainant, or a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;

G. the age of the item of communications data. Where the data includes more than one day, the recorded age of data should be the oldest date of the data sought;

H. where an item of data is service use information or traffic data retained by the CSP, an indication of the total number of days of data being sought by means of notice or authorisation; and

I. the CSP from whom the data is being acquired.

6.7. These records must be sent in written or electronic form to the Commissioner, as determined by him. Guidance on record keeping will be issued by IOCCO. Guidance may also be sought by relevant public authorities, CSPs or persons contracted by them to develop or maintain their information technology systems.

6.8. The Interception of Communications Commissioner will not seek to publish statistical information where it appears to him that doing so would be contrary to the public interest, or would be prejudicial to national security.

Records to be kept by a Communications Service Provider

6.9. To assist the Commissioner to carry out his statutory function in relation to Chapter II, CSPs should maintain a record of the disclosures it has made or been required to make. This record should be available to the Commissioner and his inspectors to enable comparative scrutiny of the records kept by public authorities. Guidance on the maintenance of records by CSPs may be issued by or sought from IOCCO.

6.10. The records to be kept by a CSP, in respect of each notice or authorisation, should include:

A. the name of the public authority;

B. the URN of the notice or authorisation;

C. the date the notice was served upon the CSP or the authorisation disclosed to the CSP;

D. a description of any communications data required where no disclosure took place or could have taken place;

E. the date when the communications data was made available to the public authority or, where secure systems are provided by the CSP, the date when the acquisition and disclosure of communications data was undertaken; and

F. sufficient records to establish the origin and exact communications data that has been disclosed in the event of later challenge in court.

Errors

6.11. Proper application of RIPA and thorough procedures for operating its provisions, including the careful preparation and checking of applications, notices and authorisations, should reduce the scope for making errors whether by public authorities or by CSPs.

6.12. An error can only occur after a designated person:

- has granted an authorisation and the acquisition of data has been initiated; or
- has given notice and the notice has been served on a CSP in writing, electronically or orally.

6.13. Any failure by a public authority to apply correctly the process of acquiring or obtaining communications data set out in this code will increase the likelihood of an error occurring.

6.14. Where any error occurs in the grant of an authorisation, the giving of a notice or as a consequence of any authorised conduct, or any conduct undertaken to comply with a notice, a record should be kept.

6.15. Where an error results in communications data being acquired or disclosed wrongly, a report must be made to the Commissioner ('a reportable error'). Such errors can have very significant consequences on an affected individual's rights with details of their private communications being disclosed to a public authority and, in extreme circumstances, being wrongly detained or wrongly accused of a crime as a result of that error.

6.16. In cases where an error has occurred but is identified by the public authority or the CSP without data being acquired or disclosed wrongly, a record will be maintained by the public authority of such occurrences ('recordable error'). These records must be available for inspection by the Commissioner.

6.17. This section of the code cannot provide an exhaustive list of possible causes of reportable or recordable errors. Examples could include:

Reportable errors

- an authorisation or notice made for a purpose, or for a type of data, which the relevant public authority cannot call upon, or seek, under RIPA;
- human error, such as incorrect transposition of information from an application to an authorisation or notice where communications data is acquired or disclosed;
- disclosure of the wrong data by a CSP when complying with a notice; and
- acquisition of the wrong data by a public authority when engaging in conduct specified in an authorisation.

Recordable errors

- a notice has been given which is impossible for a CSP to comply with and the public authority attempts to impose the requirement;
- failure to review information already held, for example unnecessarily seeking the acquisition or disclosure of data already acquired or obtained for the same investigation or operation;
- the requirement to acquire or obtain the data is known to be no longer valid;
- failure to serve written notice (or where appropriate an authorisation) upon a CSP within one working day of urgent oral notice being given or an urgent oral authorisation granted; and

- human error, such as incorrect transposition of information from an application to an authorisation or notice where communications data is not acquired or disclosed.

6.18. Reporting and recording of errors will draw attention to those aspects of the process of acquisition and disclosure of communications data that require further improvement to eliminate errors and the risk of undue interference with any individual's rights.

6.19. When a reportable error has been made, the public authority which made the error, or established that the error had been made, must establish the facts and report the error to the authority's senior responsible officer and then to the IOCCO within no more than five working days of the error being discovered. All errors should be reported as they arise. If the report relates to an error made by a CSP, the public authority should also inform the CSP and IOCCO of the report in written or electronic form. This will enable the CSP and IOCCO to investigate the cause or causes of the reported error.

6.20. The report sent to the IOCCO by a public authority in relation to a reportable error must include details of the error, identified by the public authority's unique reference number of the relevant authorisation or notice, explain how the error occurred, indicate whether any unintended collateral intrusion has taken place and provide an indication of what steps have been, or will be, taken to ensure that a similar error does not recur. When a public authority reports an error made by a CSP, the report must include details of the error and indicate whether the CSP has been informed or not (in which case the public authority must explain why the CSP has not been informed of the report).

6.21. Where a CSP discloses communications data in error, it must report each error to the IOCCO within no more than five working days of the error being discovered. It is appropriate for a person holding a suitably senior position within a CSP to do so, identifying the error by reference to the public authority's unique reference number and providing an indication of what steps have been, or will be, taken to ensure that a similar error does not recur. Errors by service providers could include responding to a notice by disclosing incorrect data or by disclosing the required data to the wrong public authority.

6.22. In circumstances where a reportable error is deemed to be of a serious nature, the Commissioner may investigate the circumstances that led to the error and assess the impact of the interference on the affected individual's rights. The Commissioner may inform the affected individual, who may make a complaint to the Investigatory Powers Tribunal (see section 9).

6.23. The records kept by a public authority accounting for recordable errors must include details of the error, explain how the error occurred and provide an indication of what steps have been, or will be, taken to ensure that a similar error does not reoccur. The authority's senior responsible officer must undertake a regular review of the recording of such errors.

6.24. Where material which has no connection or relevance to any investigation or operation undertaken by the public authority receiving it is disclosed in error by a CSP, that material and any copy of it (including copies contained in or as attachments in electronic mail) should be destroyed as soon as the report to the Commissioner has been made.

...

Excess Data

6.26. Where authorised conduct by a public authority results in the acquisition of excess data, or its disclosure by a CSP in order to comply with the requirement of a notice, all the data acquired or disclosed should be retained by the public authority.

6.27. Where a public authority is bound by the CPIA and its code of practice, there will be a requirement to record and retain data which is relevant to a criminal investigation, even if that data was disclosed or acquired beyond the scope of a valid notice or authorisation. If a criminal investigation results in proceedings being instituted all material that may be relevant must be retained at least until the accused is acquitted or convicted or the prosecutor decides not to proceed.

6.28. If, having reviewed the excess data, it is intended to make use of the excess data in the course of the investigation or operation, an applicant must set out the reason(s) for needing to use that material in an addendum to the application upon which the authorisation or notice was originally granted or given. The designated person will then consider the reason(s) and review all the data and consider whether it is necessary and proportionate for the excess data to be used in the investigation or operation. As with all communications data acquired, the requirements of the DPA and its data protection principles must also be adhered to in relation to any excess data (see next section).

7 DATA PROTECTION SAFEGUARDS

7.1. Communications data acquired or obtained under the provisions of RIPA, and all copies, extracts and summaries of it, must be handled and stored securely. In addition, the requirements of the DPA and its data protection principles must be adhered to.

7.2. Communications data that is obtained directly as a consequence of the execution of an interception warrant must be treated in accordance with the safeguards which the Secretary of State has approved in accordance with section 15 of RIPA.

Disclosure of communications data and subject access rights

7.3. This section of the code provides guidance on the relationship between disclosure of communications data under RIPA and the provisions for subject access requests under the DPA, and the balance between CSPs' obligations to comply with a notice to disclose data and individuals' right of access under section 7 of the DPA to personal data held about them.

7.4. There is no provision in RIPA preventing CSPs from informing individuals about whom they have been required by notice to disclose communications data in response to a Subject Access Request made under section 7 of the DPA. However a CSP may exercise certain exemptions to the right of subject access under Part IV of the DPA.

7.5. Section 28 of the DPA provides that data are always exempt from section 7 where such an exemption is required for the purposes of safeguarding national security.

7.6. Section 29 of the DPA provides that personal data processed for the purposes of the prevention and detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty or other imposition of a similar nature are exempt from section 7 to the extent to which the application of the provisions for rights of data subjects would be likely to prejudice any of those matters.

7.7. The exemption to subject access rights possible under section 29 does not automatically apply to the disclosure of the existence of notices given under RIPA. In the event that a CSP receives a subject access request where the fact of a disclosure under RIPA might itself be disclosed, the CSP concerned must carefully consider whether in the particular case disclosure of the fact of the notice would be likely to prejudice the prevention or detection of crime.

7.8. Where a CSP is uncertain whether disclosure of the fact of a notice would be likely to prejudice an investigation or operation, it should approach the SPoC of the public authority which gave the notice – and do so in good time to respond to the subject access request. The SPoC can make enquiries within the public authority to determine whether disclosure of the fact of the notice would likely be prejudicial to the matters in section 29.

7.9. Where a CSP withholds a piece of information in reliance on the exemption in section 28 or 29 of the DPA, it is not obliged to inform an individual that any information has been withheld. It can simply leave out that piece of information and make no reference to it when responding to the individual who has made the subject access request.

7.10. CSPs should keep a record of the steps they have taken in determining whether disclosure of the fact of a notice would prejudice the apprehension or detection of offenders. This might be useful in the event of the data controller having to respond to enquiries made subsequently by the Information Commissioner, the courts and, in the event of prejudice, the police. Under section 42 of the DPA an individual may request that the Information Commissioner assesses whether a subject access request has been handled in compliance with the DPA.

Acquisition of communication data on behalf of overseas authorities

7.11. While the majority of public authorities which obtain communications data under RIPA have no need to disclose that data to any authority outside the United Kingdom, there can be occasions when it is necessary, appropriate and lawful to do so in matters of international co‑operation.

7.12. There are two methods by which communications data, whether obtained under RIPA or not, can be acquired and disclosed to overseas public authorities:

- judicial co‑operation; or
- non‑judicial co‑operation.

Neither method compels United Kingdom public authorities to disclose data to overseas authorities. Data can only be disclosed when a United Kingdom public authority is satisfied that it is in the public interest to do so and all relevant conditions imposed by domestic legislation have been fulfilled.

Judicial co-operation

7.13. A central authority in the United Kingdom may receive a request for mutual legal assistance (MLA) which includes a request for communications data from an overseas court exercising criminal jurisdiction, an overseas prosecuting authority, or any other overseas authority that appears to have a function of making requests for MLA. This MLA request must be made in connection with criminal proceedings or a criminal investigation being carried on outside the United Kingdom, and the request for communications data included must be capable of satisfying the requirements of Part I Chapter II of RIPA.

7.14. If such an MLA request is accepted by the central authority, it will be referred for consideration by the appropriate public authority in the UK. The application may then be considered and, if appropriate, executed by that public authority under section 22 of RIPA and in line with the guidance in this code of practice.

7.15. In order for a notice or authorisation to be granted, the United Kingdom public authority must be satisfied that the application meets the same criteria of necessity and proportionality as required for a domestic application.

Non-judicial co-operation

7.16. Public authorities in the United Kingdom can receive direct requests for assistance from their counterparts in other countries. These can include requests for the acquisition and disclosure of communications data for the purpose of preventing or detecting crime. On receipt of such a request, the United Kingdom public authority may consider seeking the acquisition or disclosure of the requested data under the provisions of Chapter II of Part I of RIPA.

7.17. The United Kingdom public authority must be satisfied that the request complies with United Kingdom obligations under human rights legislation. The necessity and proportionality of each case must be considered before the authority processes the authorisation or notice.

Disclosure of communications data to overseas authorities

7.18. Where a United Kingdom public authority is considering the acquisition of communications data on behalf of an overseas authority and transferring the data to that authority, it must consider whether the data will be adequately protected outside the United Kingdom and what safeguards may be needed to ensure that. Such safeguards might include attaching conditions to the processing, storage and destruction of the data.

7.19. If the proposed transfer of data is to an authority within the European Union, that authority will be bound by the European Data Protection Directive (95/46/EC) and its national data protection legislation. Any data disclosed will be protected there without need for additional safeguards.

7.20. If the proposed transfer is to an authority outside of the European Union and the European Economic Area (Iceland, Liechtenstein and Norway), then it must not be disclosed unless the overseas authority can ensure an adequate level of data protection. The European Commission has determined that certain countries, for example Switzerland, have laws providing an adequate level of protection where data can be transferred without need for further safeguards.

7.21. In all other circumstances, the United Kingdom public authority must decide in each case, before transferring any data overseas, whether the data will be adequately protected there. The Information Commissioner has published guidance on sending personal data outside the European Economic Area in compliance with the Eighth Data Protection Principle, and, if necessary, his office can provide guidance.

7.22. The DPA recognises that it will not always be possible to ensure adequate data protection in countries outside of the European Union and the European Economic Area, and there are exemptions to the principle, for example if the transfer of data is necessary for reasons of ‘substantial public interest’. There may be circumstances when it is necessary, for example in the interests of national security, for communications data to be disclosed to a third party country, even though that country does not have adequate safeguards in place to protect the data. That is a

decision that can only be taken by the public authority holding the data on a case by case basis.

8 OVERSIGHT

8.1. RIPA provides for an Interception of Communications Commissioner ('the Commissioner') whose remit is to provide independent oversight of the exercise and performance of the powers and duties contained under Chapter II of Part I of RIPA. The Commissioner is supported by his inspectors who work from the Interception of Communications Commissioner's Office (IOCCO).

8.2. This code does not cover the exercise of the Commissioner's functions. It is the duty of any person who uses the powers conferred by Chapter II, or on whom duties are conferred, to comply with any request made by the Commissioner to provide any information he requires for the purposes of enabling him to discharge his functions.

8.3. Should the Commissioner establish that an individual has been adversely affected by any wilful or reckless failure by any person within a relevant public authority exercising or complying with the powers and duties under RIPA in relation to the acquisition or disclosure of communications data, he shall, subject to safeguarding national security, inform the affected individual of the existence of the Tribunal and its role. The Commissioner should disclose sufficient information to the affected individual to enable them to engage the Tribunal effectively.

8.4. Reports made by the Commissioner concerning the inspection of public authorities and their exercise and performance of powers under Chapter II may be made available by the Commissioner to the Home Office to promulgate good practice and help identify training requirements within public authorities and CSPs.

8.5. Subject to the approval of the Commissioner, public authorities may publish their inspection reports, in full or in summary, to demonstrate both the oversight to which they are subject and their compliance with Chapter II of RIPA and this code. Approval should be sought on a case by case basis at least ten working days prior to intended publication, stating whether the report is to be published in full, and, if not, stating which parts are to be published or how it is to be summarised."

3. News Group and Others v. The Commissioner of Police of the Metropolis IPT/14/176/H, 17 December 2015

118. These proceedings were brought before the IPT by three journalists and their employer. They challenged four authorisations issued under section 22 of RIPA with the purpose of enabling police to obtain communications data which might reveal sources of information obtained by the journalists. They argued, *inter alia*, that the section 22 regime (at the time supplemented by the 2007 Code of Practice) breached their rights under Article 10 of the Convention as it did not adequately safeguard the confidentiality of journalists' sources. The IPT agreed that the regime in place at the time did not contain effective safeguards to protect Article 10 rights in a case in which the authorisation had the purpose of obtaining disclosure of the identity of a journalist's source. It held:

"107. In the absence of a requirement for prior scrutiny by a court, particular regard must be paid to the adequacy of the other safeguards prescribed by the law. The designated person is not independent of the police force, although in practice, properly

> complying with the requirements of s 22, he will make an independent judgement, as he did in this case. In general the requirement for a decision on necessity and proportionality to be taken by a senior officer who is not involved in the investigation does provide a measure of protection as to process, but the role of the designated person cannot be equated to that of an independent and impartial judge or tribunal.
>
> 108. Subsequent oversight by the Commissioner, or, in the event of a complaint, by this Tribunal, cannot after the event prevent the disclosure of a journalist's source. This is in contrast to criminal investigations where a judge at a criminal trial may be able to exclude evidence which has been improperly or unfairly obtained by an authorisation made under s 22. Where an authorisation is made which discloses a journalist's source that disclosure cannot subsequently be reversed, nor the effect of such disclosure mitigated. Nor was there any requirement in the 2007 Code for any use of s 22 powers for the purpose of obtaining disclosure of a journalist's source to be notified to the Commissioner, so in such cases this use of the power might not be subject to any effective review. Furthermore none of the Complainants had any reason to suspect that their data had been accessed until the closing report on Operation Alice was published in September 2014. If the Respondent had not disclosed that information – and it is to his credit that he did – then the Complainants would never have been in a position to bring these proceedings.
>
> 109. So in a case involving the disclosure of a journalist's source the safeguards provided for under s 22 and the 2007 Code were limited to requiring a decision as to necessity and proportionality to be made by a senior police officer, who was not directly involved in the investigation and who had a general working knowledge of human rights law. The 2007 Code imposed no substantive or procedural requirement specific to cases affecting the freedom of the press. There was no requirement that an authorisation should only be granted where the need for disclosure was convincingly established, nor that there should be very careful scrutiny balancing the public interest in investigating crime against the protection of the confidentiality of journalistic sources. The effect of s 22 and the 2007 Code was that the designated person was to make his decision on authorisation on the basis of the same general tests of necessity and proportionality which would be applied to an application in any criminal investigation."

119. The IPT could not award any remedy in respect of the failure to provide adequate safeguards to protect Article 10 rights, as this did not in itself render the authorisations unlawful. However, it also found that one of the authorisations was unlawful, as it had been neither proportionate nor necessary. In considering the appropriate remedy, it acknowledged that it had the power to award compensation, but declined to do so since it did not consider it necessary to afford just satisfaction.

120. In March 2015 the 2007 Code of Practice was replaced by a new code. Paragraph 3.78 of that new ACD Code provides that in the specific case of an application for communications data, which is made in order to identify a journalist's source, those law enforcement agencies with powers under the Police and Criminal Evidence Act 1984 (PACE) must use the procedures of PACE to apply to a court for a production order to obtain this data.

4. The Police and Criminal Evidence Act 1984

121. Schedule 1 of PACE governs the procedure for applying to court for a production order. It provides, as relevant:

> "1. If on an application made by a constable a judge is satisfied that one or other of the sets of access conditions is fulfilled, he may make an order under paragraph 4 below.
>
> ...
>
> 4. An order under this paragraph is an order that the person who appears to the judge to be in possession of the material to which the application relates shall—
>
> (a) produce it to a constable for him to take away; or
>
> (b) give a constable access to it,
>
> not later than the end of the period of seven days from the date of the order or the end of such longer period as the order may specify.
>
> ...
>
> 7. An application for an order under paragraph 4 above that relates to material that consists of or includes journalistic material shall be made *inter partes*."

122. Section 78 of PACE permits a court to refuse to allow evidence on which the prosecution proposes to rely to be given if it appears to the court that, having regard to all the circumstances, including the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it.

D. IPT practice and procedure

1. RIPA

123. The IPT was established under section 65(1) of RIPA to hear allegations by citizens of wrongful interference with their communications as a result of conduct covered by that Act. Members must hold or have held high judicial office or be a qualified lawyer of at least ten years' standing.

124. Section 65(2) provides that the IPT is the only appropriate forum in relation to proceedings against any of the intelligence services for acts allegedly incompatible with Convention rights, and complaints by persons who allege to have been subject to the investigatory powers of RIPA. It has jurisdiction to investigate any complaint that a person's communications have been intercepted and, where interception has occurred, to examine the authority for such interception.

125. According to sections 67(2) and 67(3)(c), the IPT is to apply the principles applicable by a court on an application for judicial review. It does not, however, have power to make a Declaration of Incompatibility if it finds primary legislation to be incompatible with the European Convention

on Human Rights as it is not a "court" for the purposes of section 4 of the Human Rights Act 1998.

126. Under section 67(8), there is no appeal from a decision of the IPT "except to such extent as the Secretary of State may by order otherwise provide". No such order has been made by the Secretary of State. Furthermore, in *R(Privacy International) v. Investigatory Powers Tribunal* [2017] EWCA Civ 1868 the Court of Appeal recently confirmed that section 67(8) also had the effect of preventing a judicial review claim from being brought against a decision of the IPT. As a consequence, the IPT is a court of last resort for the purposes of the obligation to request a preliminary ruling under Article 267 of the Treaty on the Functioning of the European Union (see paragraph 236 below).

127. Section 68(6) and (7) requires those involved in the authorisation and execution of an interception warrant to disclose or provide to the IPT all documents and information it may require.

128. Section 68(4) provides that where the IPT determines any complaint it has the power to award compensation and to make such other orders as it thinks fit, including orders quashing or cancelling any warrant and orders requiring the destruction of any records obtained thereunder (section 67(7)). In the event that a claim before the IPT is successful, the IPT is generally required to make a report to the Prime Minister (section 68(5)).

129. Section 68(1) entitles the IPT to determine its own procedure, although section 69(1) provides that the Secretary of State may also make procedural rules.

2. The Investigatory Powers Tribunal Rules 2000 ("the Rules")

130. The Rules were adopted by the Secretary of State to govern various aspects of the procedure before the IPT.

131. Although the IPT is under no duty to hold oral hearings, pursuant to Rule 9 it may hold, at any stage of consideration, oral hearings at which the complainant may make representations, give evidence and call witnesses. It may also hold separate oral hearings which the person whose conduct is the subject of the complaint, the public authority against which the proceedings are brought, or any other person involved in the authorisation or execution of an interception warrant may be required to attend. Rule 9 provides that the IPT's proceedings, including any oral hearings, are to be conducted in private.

132. Rule 11 allows the IPT to receive evidence in any form, even where it would not be admissible in a court of law. It may require a witness to give evidence on oath, but no person can be compelled to give evidence at an oral hearing under Rule 9(3).

133. Rule 13 provides guidance on notification to the complainant of the IPT's findings:

> "(1) In addition to any statement under section 68(4) of the Act, the Tribunal shall provide information to the complainant in accordance with this rule.
>
> (2) Where they make a determination in favour of the complainant, the Tribunal shall provide him with a summary of that determination including any findings of fact.
>
> ...
>
> (4) The duty to provide information under this rule is in all cases subject to the general duty imposed on the Tribunal by rule 6(1).
>
> (5) No information may be provided under this rule whose disclosure would be restricted under rule 6(2) unless the person whose consent would be needed for disclosure under that rule has been given the opportunity to make representations to the Tribunal."

134. Rule 6 requires the IPT to carry out its functions in such a way as to ensure that information is not disclosed that is contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, the economic well-being of the United Kingdom or the continued discharge of the functions of any of the intelligence services. Pursuant to Rule 6, in principle, the IPT is not permitted to disclose: the fact that it has held an oral hearing under Rule 9(4); any information disclosed to it in the course of that hearing or the identity of any witness at that hearing; any information otherwise disclosed to it by any person involved in the authorisation or execution of interception warrants, or any information provided by a Commissioner; and the fact that any information has been disclosed or provided. However, the IPT may disclose such information with the consent of the person required to attend the hearing, the person who disclosed the information, the Commissioner, or the person whose consent was required for disclosure of the information, as the case may be. The IPT may also disclose such information as part of the information provided to the complainant under Rule 13(2), subject to the restrictions contained in Rule 13(4) and (5).

135. In *R(A) v. Director of Establishments of the Security Service* [2009] EWCA Civ 24 Lord Justice Laws observed that the IPT was "a judicial body of like standing and authority to the High Court". More recently, in *R(Privacy International) v. Investigatory Powers Tribunal* (cited above) Lord Justice Sales noted that "[t]he quality of the membership of the IPT in terms of judicial expertise and independence is very high".

3. IPT ruling on preliminary issues of law

136. On 23 January 2003, in a case involving a complaint by British-Irish Rights Watch, the IPT gave a ruling on preliminary issues of law, in which it considered whether a number of aspects of its procedure were within the powers conferred on the Secretary of State and Convention compliant. The IPT sat, for the first time, in public.

137. Specifically on the applicability of Article 6 § 1 to the proceedings before it, the IPT found:

> "85. The conclusion of the Tribunal is that Article 6 applies to a person's claims under section 65(2)(a) and to his complaints under section 65(2)(b) of RIPA, as each of them involves 'the determination of his civil rights' by the Tribunal within the meaning of Article 6(1)."

138. The IPT considered that Rule 9 made it clear that oral hearings could be held at its discretion. If a hearing was held, it had to be held in accordance with Rule 9. The absence from the Rules of an absolute right to either an *inter partes* oral hearing, or, failing that, to a separate oral hearing in every case was within the rule-making power in section 69(1) of RIPA and was compatible with the Convention rights under Article 6, 8 and 10. The IPT explained that oral hearings involving evidence or a consideration of the substantive merits of a claim or complaint ran the risk of breaching the "neither confirm nor deny" policy or other aspects of national security and the public interest. It was therefore necessary to provide safeguards against that and the conferring of a discretion to decide when there should be oral hearings and what form they should take was a proportionate response to the need for safeguards.

139. The IPT found the language in Rule 9(6), which stipulates that oral hearings must be held in private, to be clear and unqualified; it therefore had no discretion in the matter. It concluded that the width and blanket nature of the rule went beyond what was authorised by section 69 of RIPA and, as a consequence, it found Rule 9(6) to be *ultra vires* section 69 and not binding on it.

140. The IPT also considered the requirements in Rule 6 for the taking of evidence and disclosure. It concluded that these departures from the adversarial model were within the power conferred on the Secretary of State and compatible with Convention rights in Articles 8 and 10, taking account of the exceptions for the public interest and national security in Articles 8(2) and 10(2), and in particular the effective operation of the legitimate policy of "neither confirm nor deny" in relation to the use of investigatory powers. It noted that disclosure of information was not an absolute right where there were competing interests, such as national security considerations.

141. Finally, as regards the absence of reasons following a negative decision, the IPT concluded that section 68(4) and Rule 13 were valid and binding and that the distinction between information given to the successful complainants and that given to unsuccessful complainants (where the "neither confirm nor deny" policy had to be preserved) was necessary and justifiable.

4. Counsel to the Tribunal

142. The IPT may appoint Counsel to the Tribunal to make submissions on behalf of applicants in hearings at which they cannot be represented. In the *Liberty* case, Counsel to the Tribunal described his role as follows:

> "Counsel to the Tribunal performs a different function [from special advocates in closed proceedings conducted before certain tribunals], akin to that of *amicus curiae*. His or her function is to assist the Tribunal in whatever way the Tribunal directs. Sometimes (e.g. in relation to issues on which all parties are represented), the Tribunal will not specify from what perspective submissions are to be made. In these circumstances, counsel will make submissions according to his or her own analysis of the relevant legal or factual issues, seeking to give particular emphasis to points not fully developed by the parties. At other times (in particular where one or more interests are not represented), the Tribunal may invite its counsel to make submissions from a particular perspective (normally the perspective of the party or parties whose interests are not otherwise represented)."

143. This description was accepted and endorsed by the IPT.

E. Oversight

144. Part IV of RIPA provided for the appointment by the Prime Minister of an Interception of Communications Commissioner and an Intelligence Services Commissioner charged with supervising the activities of the intelligence services.

145. The Interception of Communications Commissioner was responsible for keeping under review the interception of communications and the acquisition and disclosure of communications data by intelligence agencies, police forces and other public authorities. He reported to the Prime Minister on a half-yearly basis with respect to the carrying out of his functions. This report was a public document (subject to the non-disclosure of confidential annexes) which was laid before Parliament. In undertaking his review of surveillance practices, the Commissioner and his inspectors had access to all relevant documents, including closed materials, and all those involved in interception activities had a duty to disclose to him any material he required. The obligation on intercepting agencies to keep records ensured that the Commissioner had effective access to details of surveillance activities undertaken.

146. The Intelligence Services Commissioner also provided independent external oversight of the use of the intrusive powers of the intelligence services and parts of the Ministry of Defence. He also submitted annual reports to the Prime Minister, which were laid before Parliament.

147. However, these provisions, insofar as they relate to England, Scotland and Wales, were repealed by the Investigatory Powers Act 2016 (see paragraphs 195-201 below) and in September 2017 the Investigatory Powers Commissioner's Office ("IPCO") took over responsibility for the

oversight of investigatory powers. The IPCO consists of around fifteen Judicial Commissioners, current and recently retired High Court, Court of Appeal and Supreme Court Judges; a Technical Advisory Panel made up of scientific experts; and almost fifty official staff, including inspectors, lawyers and communications experts. The more intrusive powers such as interception, equipment interference and the use of surveillance in sensitive environments will be subject to the prior approval of a Judicial Commissioner once the provisions of the 2016 Act have entered into force. Use of these and other surveillance powers, including the acquisition of communications data and the use of covert human intelligence sources, are also overseen by a programme of retrospective inspection and audit by Judicial Commissioners and IPCO's inspectors.

F. Reviews of interception operations by the intelligence service

1. *Intelligence and Security Committee of Parliament: July 2013 Statement on GCHQ's alleged interception of communications under the US PRISM programme*

148. The Intelligence and Security Committee of Parliament ("the ISC") was originally established by the Intelligence Services Act 1994 to examine the policy, administration and expenditure of MI5, MI6, and GCHQ. Since the introduction of the Justice and Security Act 2013, however, the ISC was expressly given the status of a Committee of Parliament; was provided with greater powers; and its remit was increased to include *inter alia* oversight of operational activity and the wider intelligence and security activities of Government. Pursuant to sections 1-4 of the Justice and Security Act 2013, it consists of nine members drawn from both Houses of Parliament, and, in the exercise of their functions, those members are routinely given access to highly classified material in carrying out their duties.

149. Following the Edward Snowden revelations, the ISC conducted an investigation into GCHQ's access to the content of communications intercepted under the US PRISM programme, the legal framework governing access, and the arrangements GCHQ had with its overseas counterpart for sharing information. In the course of the investigation, the ISC took detailed evidence from GCHQ and discussed the programme with the NSA.

150. The ISC concluded that allegations that GCHQ had circumvented United Kingdom law by using the NSA PRISM programme to access the content of private communications were unfounded as GCHQ had complied with its statutory duties contained in the ISA. It further found that in each case where GCHQ sought information from the United States, a warrant for interception, signed by a Government Minister, had already been in place. However, it found it necessary to further consider whether the current

statutory framework governing access to private communications remained accurate.

2. Privacy and security: a modern and transparent legal framework

151. Following its statement in July 2013, the ISC conducted a more in-depth inquiry into the full range of the intelligence services' capabilities. Its report, which contained an unprecedented amount of information about the intelligence services' intrusive capabilities, was published on 12 March 2015 (see paragraphs 11-13 above).

152. The ISC was satisfied that the United Kingdom's intelligence and security services did not seek to circumvent the law, including the requirements of the Human Rights Act 1998, which governs everything that they do. However, it considered that as the legal framework had developed piecemeal, it was unnecessarily complicated. The ISC therefore had serious concerns about the resulting lack of transparency, which was not in the public interest. Consequently, its key recommendation was that the current legal framework be replaced by a new Act of Parliament which should clearly set out the intrusive powers available to the intelligence services, the purposes for which they may use them, and the authorisation required before they may do so.

153. With regard to GCHQ's bulk interception capability, the inquiry showed that the intelligence services did not have the legal authority, the resources, the technical capability, or the desire to intercept every communication of British citizens, or of the Internet as a whole: thus, GCHQ were not reading the emails of everyone in the United Kingdom. On the contrary, GCHQ's bulk interception systems operated on a very small percentage of the bearers that made up the Internet and the ISC was satisfied that GCHQ applied levels of filtering and selection such that only a certain amount of the material on those bearers was collected. Further targeted searches ensured that only those items believed to be of the highest intelligence value were ever presented for analysts to examine, and therefore only a tiny fraction of those collected were ever seen by human eyes.

154. In respect of Internet communications, the ISC considered that the current system of 'internal' and 'external' communications was confusing and lacked transparency and it therefore suggested that the Government publish an explanation of which Internet communications fall under which category, including a clear and comprehensive list of communications.

155. Nevertheless, the inquiry had established that bulk interception could not be used to target the communications of an individual in the United Kingdom without a specific authorisation naming that individual, signed by a Secretary of State.

156. With regard to section 8(4) warrants, the ISC observed that the warrant itself was very brief. It further noted that insofar as the

accompanying certificate set out the categories of communications which might be examined, those categories were expressed in very general terms (for example, "material providing intelligence on terrorism (as defined by the Terrorism Act 2000 (as amended)), including, but not limited to, terrorist organisations, terrorists, active sympathisers, attack planning, fund-raising"). Given that the certificate was so generic, the ISC questioned whether it needed to be secret or whether, in the interests of transparency, it could be published.

157. Although the section 8(4) certificate set out the general categories of information which might be examined, the ISC observed that in practice, it was the selection of the bearers, the application of simple selectors and initial search criteria, and then complex searches which determined what communications were examined. The ISC had therefore sought assurances that these were subject to scrutiny and review by Ministers and/or the Commissioners. However, the evidence before the ISC indicated that neither Ministers nor the Commissioners had any significant visibility of these issues. The ISC therefore recommended that the Interception of Communications Commissioner should be given statutory responsibility to review the various selection criteria used in bulk interception to ensure that they followed directly from the Certificate and valid national security requirements.

158. The ISC noted that communications data was central to most intelligence services' investigations: it could be analysed to find patterns that reflected particular online behaviours associated with activities such as attack planning, and to establish links, to help focus on individuals who might pose a threat, to ensure that interception was properly targeted, and to illuminate networks and associations relatively quickly. It was particularly useful in the early stages of an investigation, when the intelligence services had to be able to determine whether those associating with a target were connected to the plot (and therefore required further investigation) or were innocent bystanders. According to the Secretary of State for the Home Department, it had "played a significant role in every Security Service counter-terrorism operation over the last decade". Nevertheless, the ISC expressed concern about the definition of "communications data". While it accepted that there was a category of communications data which was less intrusive than content, and therefore did not require the same degree of protection, it considered that there now existed certain categories of communications data which had the potential to reveal more intrusive details about a person's private life and, therefore, required greater safeguards.

159. Finally, with regard to the IPT, it expressly recognised the importance of a domestic right of appeal.

3. "A Question of Trust": Report of the Investigatory Powers Review by the Independent Reviewer of Terrorism Legislation ("the Anderson Report")

160. The Independent Reviewer of Terrorism Legislation, a role that has existed since the late 1970s, is an independent person, appointed by the Home Secretary and by the Treasury for a renewable three-year term and tasked with reporting to the Home Secretary and to Parliament on the operation of counter-terrorism law in the United Kingdom. These reports are then laid before Parliament, to inform the public and political debate. The Independent Reviewer's role is to inform the public and political debate on anti-terrorism law in the United Kingdom. The uniqueness of the role lies in its complete independence from government, coupled with access based on a very high degree of clearance to secret and sensitive national security information and personnel.

161. The purpose of the Anderson Report, published in June 2015 and identified by reference to the then Independent Reviewer of Terrorism Legislation, was to inform the public and political debate on the threats to the United Kingdom, the capabilities required to combat those threats, the safeguards in place to protect privacy, the challenges of changing technology, issues relating to transparency and oversight, and the case for new or amended legislation. In conducting the review the Independent Reviewer had unrestricted access, at the highest level of security clearance, to the responsible Government departments and public authorities. He also engaged with service providers, independent technical experts, non-governmental organisations, academics, lawyers, judges and regulators.

162. The Independent Reviewer noted that the statutory framework governing investigatory powers had developed in a piecemeal fashion, with the consequence that there were "few [laws] more impenetrable than RIPA and its satellites".

163. With regard to the importance of communications data, he observed that it enabled the intelligence services to build a picture of a subject of interest's activities and was extremely important in providing information about criminal and terrorist activity. It identified targets for further work and also helped to determine if someone was completely innocent. Of central importance was the ability to use communications data (subject to necessity and proportionality) for:

(a) linking an individual to an account or action (for example, visiting a website, sending an email) through IP resolution;

(b) establishing a person's whereabouts, traditionally via cell site or GPRS data;

(c) establishing how suspects or victims are communicating (that is, via which applications or services);

(d) observing online criminality (for example, which websites are being visited for the purposes of terrorism, child sexual exploitation or purchases of firearms or illegal drugs); and

(e) exploiting data (for example, to identify where, when and with whom or what someone was communicating, how malware or a denial of service attack was delivered, and to corroborate other evidence).

164. Moreover, analysis of communications data could be performed speedily, making it extremely useful in fast-moving operations, and use of communications data could build a case for using a more intrusive measure, or deliver the information that would make other measures unnecessary.

165. His proposals for reform can be summarised as follows:

(a) A comprehensive and comprehensible new law should be drafted, replacing "the multitude of current powers" and providing clear limits and safeguards on any intrusive power it may be necessary for public authorities to use;

(b) The definitions of "content" and "communications data" should be reviewed, clarified and brought up-to-date;

(c) The capability of the security and intelligence agencies to practice bulk collection of intercepted material and associated communications data should be retained, but only subject to strict additional safeguards including the authorisation of all warrants by a Judicial Commissioner at a new Independent Surveillance and Intelligence Commission ("ISIC");

(d) The purposes for which material or data was sought should be spelled out in the accompanying certificate by reference to specific operations or mission purposes (for example, "attack planning by ISIL in Iraq/Syria against the UK");

(e) There should be a new form of bulk warrant limited to the acquisition of communications data which could be a proportionate option in certain cases;

(f) Regarding the authorisation for the acquisition of communications data, designated persons should be required by statute to be independent from the operations and investigations in relation to which the authorisation is sought;

(g) Novel or contentious requests for communications data, or requests for the purpose of determining matters that are privileged or confidential, should be referred to the ISIC for determination by a Judicial Commissioner;

(h) The ISIC should take over intelligence oversight functions and should be public-facing, transparent and accessible to the media; and

(i) The IPT should have the capacity to make declarations of incompatibility and its rulings should be subject to appeals on points of law.

4. A Democratic Licence to Operate: Report of the Independent Surveillance Review ("ISR")

166. The ISR was undertaken by the Royal United Services Institute, an independent think-tank, at the request of the then deputy Prime Minister, partly in response to the revelations by Edward Snowden. Its terms of reference were to look at the legality of United Kingdom surveillance programmes and the effectiveness of the regimes that govern them, and to suggest reforms which might be necessary to protect both individual privacy and the necessary capabilities of the police and security and intelligence services.

167. Despite the revelations by Edward Snowden, having completed its review the ISR found no evidence that the British Government was knowingly acting illegally in intercepting private communications, or that the ability to collect data in bulk was being used by the Government to provide it with a perpetual window into the private lives of British citizens. On the other hand, it found evidence that the present legal framework authorising the interception of communications was unclear, had not kept pace with developments in communications' technology, and did not serve either the Government or members of the public satisfactorily. It therefore concluded that a new, comprehensive and clearer legal framework was required.

168. In particular, it supported the view set out in both the ISC and Anderson reports that while the current surveillance powers were needed, both a new legislative framework and oversight regime were required. It further considered that the definitions of "content" and "communications data" should be reviewed as part of the drafting of the new legislation so that they could be clearly delineated in law.

169. With regard to communications data, the report noted that greater volumes were available on an individual relative to content, since every piece of content was surrounded by multiple pieces of communications data. Furthermore, aggregating data sets could create an extremely accurate picture of an individual's life since, given enough raw data, algorithms and powerful computers could generate a substantial picture of the individual and his or her patterns of behaviour without ever accessing content. In addition, the use of increasingly sophisticated encryption methods had made content increasingly difficult to access.

170. It further considered that the capability of the security and intelligence services to collect and analyse intercepted material in bulk should be maintained, but with the stronger safeguards recommended in the Anderson Report. In particular, it agreed that warrants for bulk interception should include much more detail than is currently the case and should be the subject of a judicial authorisation process, save for when there is an urgent requirement.

171. In addition, it agreed with both the ISC and the Anderson report that there should be different types of warrant for the interception and acquisition of communications and related data. It was proposed that warrants for a purpose relating to the detection or prevention of serious and authorised crime should always be authorised by a Judicial Commissioner, while warrants for purposes relating to national security should be authorised by the Secretary of State subject to judicial review by a Judicial Commissioner.

172. With regard to the IPT, the ISR recommended open public hearings, except where it was satisfied private or closed hearings were necessary in the interests of justice or other identifiable public interest. Furthermore, it should have the ability to test secret evidence put before it, possibly through the appointment of Special Counsel. Finally, it agreed with the ISC and Anderson reports that a domestic right of appeal was important and should be considered in future legislation.

5. Report of the Bulk Powers Review

173. The bulk powers review was set up in May 2016 to evaluate the operational case for the four bulk powers contained in what was then the Investigatory Powers Bill (now the Investigatory Powers Act 2016: see paragraphs 195-201 below). Those powers related to bulk interception and the bulk acquisition of communications data, bulk equipment interference and the acquisition of bulk personal datasets.

174. The review was again carried out by the Independent Reviewer of Terrorism Legislation. To conduct the review he recruited three team members, all of whom had the necessary security clearance to access very highly classified material, including a person with the necessary technical background to understand the systems and techniques used by GCHQ, and the uses to which they could be put; an investigator with experience as a user of secret intelligence, including intelligence generated by GCHQ; and senior independent counsel with the skills and experience to challenge forensically the evidence and the case studies presented by the security and intelligence services.

175. In conducting their review, the team had significant and detailed contact with the intelligence services at all levels of seniority as well as the relevant oversight bodies (including the IPT and Counsel to the Tribunal in the relevant cases), NGOs and independent technical experts.

176. Although the review was of the Investigatory Powers Bill, a number of its findings in respect of bulk interception are relevant to the case at hand. In particular, having examined a great deal of closed material, the review concluded that it was an essential capability: first, because terrorists, criminal and hostile foreign intelligence services had become increasingly sophisticated at evading detection by traditional means; and secondly, because the nature of the global Internet meant that the route a particular

communication would travel had become hugely unpredictable. The review team looked at alternatives to bulk interception (including targeted interception, the use of human sources and commercial cyber-defence products) but concluded that no alternative or combination of alternatives would be sufficient to substitute for the bulk interception power as a method of obtaining the necessary intelligence.

6. Attacks in London and Manchester March-June 2017: Independent Assessment of MI5 and Police Internal Reviews

177. Following a series of four terrorist attacks in the short period between March and June 2017, in the course of which some 36 innocent people were killed and almost 200 more were injured, the Home Secretary asked the recently retired Independent Reviewer of Terrorism Legislation, David Anderson Q.C. to assess the classified internal reviews of the police and intelligence services involved. In placing the attacks in context, the Report made the following observations:

> "1.2 The attacks under review were the most deadly terrorist attacks on British soil since the 7/7 London tube and bus bombings of July 2005. All four were shocking for their savagery and callousness. The impact of the first three attacks was increased by the fact that they came at the end of a long period in which Islamist terrorism had taken multiple lives in neighbouring countries such as France, Belgium and Germany but had not enjoyed equivalent success in Britain.
>
> 1.3 The plots were part of an increasingly familiar pattern of Islamist and (to a lesser extent) anti-Muslim terrorist attacks in western countries, including in particular northern Europe. The following points provide context, and an indication that lessons learned from these incidents are likely to be transferrable.
>
> 1.4 First, the ***threat level*** in the UK from so-called "international terrorism" (in practice, Islamist terrorism whether generated at home or abroad) has been assessed by the Joint Terrorism Analysis Centre (JTAC) as SEVERE since August 2014, indicating that Islamist terrorist attacks in the UK are "highly likely". Commentators with access to the relevant intelligence have always been clear that this assessment is realistic. They have pointed also to the smaller but still deadly threat from extreme right wing (XRW) terrorism, exemplified by the murder of Jo Cox MP in June 2016 and by the proscription of the neo-Nazi group National Action in December 2016.
>
> 1.5 Secondly, the ***growing scale*** of the threat from Islamist terrorism is striking. The Director General of MI5, Andrew Parker, spoke in October 2017 of "a dramatic upshift in the threat this year" to "the highest tempo I've seen in my 34 year career". Though deaths from Islamist terrorism occur overwhelmingly in Africa, the Middle East and South Asia, the threat has grown recently across the western world, and has been described as "especially diffuse and diverse in the UK". It remains to be seen how this trend will be affected, for good or ill, by the physical collapse of the so-called Islamic State in Syria and Iraq.
>
> 1.6 Thirdly, the profiles of the ***attackers*** ... display many familiar features. Comparing the five perpetrators of the Westminster, Manchester and London Bridge attacks with those responsible for the 269 Islamist-related terrorist offences in the UK between 1998-2015, as analysed by Hannah Stuart ("the total"):

(a) All were ***male***, like 93% of the total.

(b) Three were ***British*** (Masood, Abedi, Butt), like 72% of the total.

(c) One was a ***convert to Islam*** (Masood), like 16% of the total.

(d) Three ***resided*** in London (43% of the total) and one in North West England (10% of the total).

(e) Three (Masood, and to a more limited extent Abedi and Butt) were ***known to the police***, like 38% of the total.

(f) The same three were ***known to MI5***, like 48% of the total.

(g) At least one (Butt) had direct links to a ***proscribed terrorist organisation***, as had 44% of the total. His links, in common with 56% of the total who had links with such organisations, were with ***Al-Muhajiroun*** (ALM).

In view of their possible pending trials I say nothing of Hashem Abedi, currently detained in Libya in connection with the Manchester attack, or of the Finsbury Park attacker Darren Osborne who (like Khalid Masood at Westminster) is not alleged to have had accomplices.

1.7 Fourthly, though the ***targets*** of the first three attacks did not extend to the whole of the current range, they had strong similarities to the targets of other recent western attacks: political centres (e.g. Oslo 2011, Ottawa 2014, Brussels 2016); concert-goers, revellers and crowds (e.g. Orlando 2016, Paris 2016, Barcelona 2017); and police officers (e.g. Melbourne 2014, Berlin 2015, Charleroi 2016). There are precedents also for attacks on observant Muslims which have crossed the boundary from hate crime to terrorism, including the killing of Mohammed Saleem in the West Midlands in 2013.

1.8 Fifthly, the ***modus operandi*** (MO) of terrorist attacks has diversified and simplified over the years, as Daesh has employed its formidable propaganda effort to inspire rather than to direct acts of terrorism in the west. The attacks under review were typical in style for their time and place:

(a) Unlike the large, directed Islamist plots characteristic of the last decade, all four attacks were committed by ***lone actors*** or ***small groups***, with little evidence of detailed planning or precise targeting.

(b) Strong gun controls in the UK mean that ***bladed weapons*** are more commonly used than firearms in gang-related and terrorist crime.

(c) Since a truck killed 86 innocent people in Nice (July 2016), ***vehicles*** – which featured in three of the four attacks under review – have been increasingly used as weapons.

(d) The ***combination*** of a vehicle and bladed weapons, seen at Westminster and London Bridge, had previously been used to kill the soldier Lee Rigby (Woolwich, 2013).

(e) ***Explosives***, used in Manchester, were the most popular weapon for Islamist terrorists targeting Europe between 2014 and 2017. The explosive TATP has proved to be capable of manufacture (aided by on-line purchases and assembly instructions) more easily than was once assumed."

7. Annual Report of the Interception of Communications Commissioner for 2016

(a) Section 8(4) warrants

178. The Commissioner observed that when conducting interception under a section 8(4) warrant, an intercepting agency had to use its knowledge of the way in which international communications were routed, combined with regular surveys of relevant communications links, to identify those individual communications bearers that were most likely to contain external communications that would meet the descriptions of material certified by the Secretary of State under section 8(4). It also had to conduct the interception in ways that limited the collection of non-external communications to the minimum level compatible with the objective of intercepting the wanted external communications.

179. He further observed that prior to analysts being able to read, look at or listen to material, they had to provide a justification, which included why access to the material was required, consistent with, and pursuant to section 16 and the applicable certificate, and why such access was proportionate. Inspections and audits showed that although the selection procedure was carefully and conscientiously undertaken, it relied on the professional judgment of analysts, their training and management oversight.

180. According to the report, 3007 interception warrants were issued in 2016 and five applications were refused by a Secretary of State. In the view of the Commissioner, these figures did not capture the critical quality assurance function initially carried out by the staff and lawyers within the intercepting agency or the warrant-granting department (the warrant-granting departments were a source of independent advice to the Secretary of State and performed pre-authorisation scrutiny of warrant applications and renewals to ensure that they were (and remained) necessary and proportionate). Based on his inspections, he was confident that the low number of rejections reflected the careful consideration given to the use of these powers.

181. A typical inspection of an interception agency included the following:

- 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 were sufficient for the purposes of Chapter 1 of Part 1 of RIPA and that all relevant records had been kept;
- the 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 investigations or operations to assess whether the interception and the justifications for acquiring all of the material were proportionate;
- the examination of any urgent oral approvals to check that the process was justified and used appropriately;
- a review of those cases where communications subject to legal privilege or otherwise confidential information had been intercepted and retained, and any cases where a lawyer was the subject of an investigation;
- a review of the adequacy of the safeguards and arrangements under sections 15 and 16 of RIPA;
- an investigation of the procedures in place for the retention, storage and destruction of intercepted material and related communications data; and
- a review of the errors reported, including checking that the measures put in place to prevent recurrence were sufficient.

182. After each inspection, inspectors produced a report, including:

- an assessment of how far the recommendations from the previous inspection had been achieved;
- a summary of the number and type of interception documents selected for inspection, including a detailed list of those warrants;
- detailed comments on all warrants selected for further examination and discussion during the inspection;
- an assessment of the errors reported to the Commissioner's office during the inspection period;
- an account of the examination of the retention, storage and destruction procedures;
- an account of other policy or operational issues which the agency or warrant-granting departments raised during the inspection;
- an assessment of how any material subject to legal professional privilege (or otherwise confidential material) has been handled;
- a number of recommendations aimed at improving compliance and performance.

183. During 2016, the Commissioner's office inspected all nine interception agencies once and the four main warrant-granting departments twice. This, together with extra visits to GCHQ, made a total of twenty-two inspection visits. In addition, he and his inspectors arranged other *ad hoc* visits to agencies.

184. Inspection of the systems in place for applying for and authorising interception warrants usually involved a three-stage process. First, to achieve a representative sample of warrants, inspectors selected them across different crime types and national security threats. In addition, inspectors

focussed on those of particular interest or sensitivity (such as those which gave rise to an unusual degree of collateral intrusion, those which have been extant for a considerable period, those which were approved orally, those which resulted in the interception of legal or otherwise confidential communications, and so-called 'thematic' warrants). Secondly, inspectors scrutinised the selected warrants and associated documentation in detail during reading days which preceded the inspections. Thirdly, they identified those warrants, operations or areas of the process which required further information or clarification and arranged to interview relevant operational, legal or technical staff. Where necessary, they examined further documentation or systems relating to those warrants.

185. 970 warrants were examined during the twenty-two interception inspections (sixty-one percent of the number of warrants in force at the end of the year and thirty-two percent of the total of new warrants issued in 2016).

186. According to the report, every interception agency had a different view on what constituted an appropriate retention period for intercepted material and related communications data. There was no period prescribed by the legislation, but the agencies had to consider section 15(3) of RIPA, which provided that the material or data had to be destroyed as soon as retaining it was no longer necessary for any of the authorised purposes in section 15(4). The vast majority of content was reviewed and automatically deleted after a very short period of time unless specific action was taken to retain the content for longer because it was necessary to do so. The retention periods differed within the interception agencies and ranged between thirty days and one year. The retention periods for related communications data also differed within the interception agencies, but ranged between six months and one year.

187. Inspectors made a total of twenty-eight recommendations in their inspection reports, eighteen of which were made in relation to the application process. The majority of the recommendations in this category related to the necessity, proportionality and/or collateral intrusion justifications in the applications; or the handling of legally privileged or otherwise confidential material relating to sensitive professions.

188. The total number of interception errors reported to the Commissioner during 2016 was 108. Key causes of interception errors were over-collection (generally technical software or hardware errors that caused over-collection of intercepted material and related communications data), unauthorised selection/examination, incorrect dissemination, the failure to cancel interception, and the interception of either an incorrect communications address or person.

(b) Acquisition of communications data under Chapter II of RIPA

189. According to the report, police forces and law enforcement agencies were responsible for acquiring ninety-three percent of the total number of items of data in 2016, six percent was acquired by intelligence services and the remaining one percent was acquired by other public authorities, including local authorities. Fifty percent of the data acquired was subscriber information, forty-eight percent was traffic data and two percent service use information. Most of the acquired items of data (eighty-one percent) related to telephony, such as landlines or mobile phones. Internet identifiers, for example email or IP addresses, accounted for fifteen percent of the acquired data and two percent of requests were related to postal identifiers.

190. With regard to the purpose of the request, eighty-three percent of the items of data were acquired for the purpose of preventing or detecting crime or preventing disorder; eleven percent were acquired for the purpose of preventing death or injury or damage to a person's mental health, or of mitigating any injury or damage to a person's physical or mental health; and six percent were acquired in the interests of national security.

191. Furthermore, approximately seventy percent of data requests were for data less than three months old, twenty-five percent aged between three months and one year, and six percent for data over twelve months old. Eighty-one percent of the requests required data for a communications address for periods of three months or less (for example, three months of incoming and outgoing call data for a communications address). Twenty-five percent of all requests were for data relating to a period of less than one day.

192. Twenty-seven percent of submitted applications were returned to the applicant by the Single Point of Contact ("SPoC") for development and a further five percent were declined by the SPoC. Reasons for refusing data applications included: lack of clarity; failure to link the crime to the communications address; and insufficient justification for collateral intrusion. Four percent of submitted applications were returned to applicants by designated persons for further development and one percent was rejected. The main reason for designated persons returning or rejecting applications was that they were not satisfied with the necessity or proportionality justifications given (fifty-two percent). A significant number of applications were returned because designated persons were not satisfied with the overall quality or clarity of the application (twenty-one percent). Other reasons for rejection included the designated persons declaring that they were not independent of the investigation and requesting that the application be forwarded to an independent designated person for consideration (six percent).

193. In 2016 forty-seven public authorities advised that they had made a total of 948 applications that related to persons who were members of

sensitive professions. A significant proportion of these 948 applications were categorised incorrectly (that is, the applicant had recorded a sensitive profession when there was not one). This was usually because the applicant erred on the side of caution, recording a sensitive profession if there was a possibility of one, rather than because they knew that there was one, a fact which provided the Commissioner with "a greater level of assurance that [designated persons] are taking sensitive professions into account when necessary". Furthermore, according to the Commissioner, most applications relating to members of sensitive professions were submitted because the individual had been a victim of crime or was the suspect in a criminal investigation. In these cases, the profession of the individual was usually not relevant to the investigation, but public authorities showed proper consideration of the sensitive profession by bringing it to the attention of the authorising officer.

194. Having considered the "reportable errors", the Commissioner noted that the number of serious errors remained very low (0.004%).

G. The Investigatory Powers Act 2016

195. The Investigatory Powers Act 2016 received Royal Assent on 29 November 2016.

196. On 30 December 2016 Part 4 of the 2016 Act, which included a power to issue "retention notices" to telecommunications operators requiring the retention of data, came into force (although not in its entirety). Following a legal challenge by Liberty, the Government conceded that Part 4 of the IPA was, in its current form, inconsistent with the requirements of EU law. Part 4 was not amended and on 27 April 2018 the High Court found Part 4 to be incompatible with fundamental rights in EU law since, in the area of criminal justice, access to retained data was not limited to the purpose of combating "serious crime"; and access to retained data was not subject to prior review by a court or an independent administrative body. The court concluded that the legislation had to be amended by 1 November 2018.

197. On 13 February 2017 the provisions of the IPA relating to the appointment of the Investigatory Powers Commissioner and other Judicial Commissioners came into force. On 3 March 2017, the Government appointed the first Investigatory Powers Commissioner (a judge currently sitting on the Court of Appeal and former justice of the International Criminal Court) for a three-year term and he took up appointment with immediate effect. The newly created Investigatory Powers Commissioners Office ("ICPO") commenced operations on 8 September 2017 and is ultimately due to consist of around 70 staff (including approximately fifteen judicial commissioners made up of current and recently retired judges of the

High Court, Court of Appeal and Supreme Court, and a technical advisory panel of scientific experts).

198. The remainder of the 2016 Act is not yet in force.

199. In terms of safeguards, when it enters into force in full the Act will require that bulk interception and bulk equipment interference warrants may only be issued where the main purpose of the interception is to acquire intelligence relating to individuals outside the United Kingdom, even where the conduct occurs within the United Kingdom. Similarly, interference with the privacy of persons in the United Kingdom will be permitted only to the extent that it is necessary for that purpose. It will also introduce a "double-lock" for the most intrusive surveillance powers, meaning that a warrant issued by the Secretary of State will also require the approval of one of the appointed Judicial Commissioners. There will also be new protections for journalistic and legally privileged material, including a requirement for judicial authorisation for the acquisition of communications data identifying journalists' sources; tough sanctions for the misuse of powers, including the creation of new criminal offences; and a right of appeal from the IPT.

200. In addition, the new Act will consolidate and update the powers available to the State to obtain communications and communications data. It will provide an updated framework for the use (by the security and intelligence services, law enforcement and other public authorities) of investigatory powers to obtain communications and communications data. These powers cover the interception of communications, the retention and acquisition of communications data, and equipment interference for obtaining communications and other data. The Act also makes provision relating to the security and intelligence services' retention and examination of bulk personal datasets.

201. On 23 February 2017 the Home Office launched a public consultation on the five draft codes of practice it intends to issue under the 2016 Act (on the Interception of Communications, Equipment Interference, Bulk Communications Data Acquisition, Retention and Use of Bulk Personal Datasets by the Security and Intelligence Agencies and National Security Notices), which will set out the processes and safeguards governing the use of investigatory powers by public authorities. They will give detail on how the relevant powers should be used, including examples of best practice. They are intended to provide additional clarity and to ensure the highest standards of professionalism and compliance with the relevant legislation. Following the closure of the consultation on 6 April 2017, the draft codes were further amended and Regulations bringing them into force will be laid and debated before Parliament. They will only come into force when they have been debated in both Houses of Parliament and approved by a resolution in both Houses.

H. Relevant international law

1. The United Nations

(a) Resolution no. 68/167 on The Right to Privacy in the Digital Age

202. Resolution no. 68/167, adopted by the General Assembly on 18 December 2013, reads as follows:

> "The General Assembly,
>
> ...
>
> 4. *Calls upon* all States:
>
> ...
>
> (*c*) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;
>
> (*d*) To establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data ..."

(b) The Constitution of the International Telecommunication Union 1992

203. Articles 33 and 37 of the Constitution provide as follows:

The Right of the Public to Use the International Telecommunication Service

"Member States recognize the right of the public to correspond by means of the international service of public correspondence. The services, the charges and the safeguards shall be the same for all users in each category of correspondence without any priority or preference.
..."

Secrecy of Telecommunications

> "1. Member States agree to take all possible measures, compatible with the system of telecommunication used, with a view to ensuring the secrecy of international correspondence.

2. Nevertheless, they reserve the right to communicate such correspondence to the competent authorities in order to ensure the application of their national laws or the execution of international conventions to which they are parties."

(c) The 2006 Annual Report of the International Law Commission

204. In its 2006 Annual Report the ILC proposed to include the topic "Protection of personal data in the transborder flow of information" in its

long-term programme of work. The Secretariat's supporting report (Annex D) identifies a number of core principles of public international law:

Core principles

"23. A number of core principles are discernible from developments in this field in almost forty-years. Such principles include the following:

Lawful and fair data collection and processing: This principle presupposes that the collection of personal data would be restricted to a necessary minimum. In particular such data should not be obtained unlawfully or through unfair means;

Accuracy: The information quality principle is a qualitative requirement and entails a responsibility that the data be accurate, and necessarily complete and up to date for the purpose intended.

Purpose specification and limitation: This principle establishes the requirement that the purpose for which the data are collected should be specified to the data subject. Data should not be disclosed, made available or otherwise used for purposes other than those specified. It has to be done with the consent or knowledge of the data-subject or under the operation of the law. Any subsequent use is limited to such purpose, or any other that is not incompatible with such purpose. Differences lie in the approaches taken by States. Some jurisdictions perceive the obligation for consent to be ex ante.

Proportionality: Proportionality requires that the necessary measure taken should be proportionate to the legitimate claims being pursued.

Transparency: Denotes a general policy of openness regarding developments, practices and policies with respect to protection of personal data.

Individual participation and in particular the right to access: This principle may be the most important for purposes of data protection. The individual should have access to such data; as well as to the possibility of determining whether or not the keeper of the file has data concerning him; to obtain such information or to have it communicated to him in a form, in a manner and at a cost that is reasonable. This accords with the right of an individual to know about the existence of any data file, its contents, to challenge the data and to have it corrected, amended or erased.

Non-discrimination: This principle connotes that data likely to give rise to unlawful and arbitrary discrimination should not be compiled. This includes information collated on racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union.

Responsibility: This principle embraces data security; data should be protected by reasonable and appropriate measures to prevent their loss, destruction, unauthorized access, use, modification or disclosure and the keeper of the file should be accountable for it.

Independent supervision and legal sanction: Supervision and sanction require that there should be a mechanism for ensuring due process and accountability. There should be an authority accountable in law for giving effect to the requirements of data protection.

Data equivalency in the case of transborder flow of personal data: This is a principle of compatibility; it is intended to avoid the creation of unjustified obstacles and restrictions to the free flow of data, as long as the circulation is consistent with the standard or deemed adequate for that purpose.

The principle of derogability: This entails power to make exceptions and impose limitations if they are necessary to protect national security, public order, public health or morality or to protect the rights of others."

Derogability

"24. While privacy concerns are of critical importance, such concerns have to be balanced with other value-interests. The privacy values to avoid embarrassment, to

construct intimacy and to protect against misuse associated with the need to protect the individual have to be weighed against other counter-values against individual control over personal information; such as the need not to disrupt the flow of international trade and commerce and the flow of information; the importance of securing the truth, as well as the need to be live in secure environment. There are allowable restrictions and exceptions, for example, with respect to national security, public order (ordre public), public health or morality or in order to protect the rights and freedoms of others, as well as the need for effective law enforcement and judicial cooperation in combating crimes at the international level, including the threats posed by international terrorism and organized crime.

25. The processing of personal data must be interpreted in accordance with human rights principles. Accordingly, any of the objectives in the public interest would justify interference with private life if it is (a) in accordance with the law, (b) is necessary in a democratic society for the pursuit of legitimate aims, and (c) is not disproportionate to the objective pursued. The phrase "in accordance with the law" goes beyond to the formalism of having in existence a legal basis in domestic law, it requires that the legal basis be "accessible" and foreseeable". Foreseeability necessitates sufficiency of precision in formulation of the rule to enable any individual to regulate his conduct."

2. The Council of Europe

(a) The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981

205. The Convention, which entered into force in respect of the United Kingdom on 1 December 1987, sets out standards for data protection in the sphere of automatic processing of personal data in the public and private sectors. It provides, insofar as relevant:

Preamble

"The member States of the Council of Europe, signatory hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;

Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing;

Reaffirming at the same time their commitment to freedom of information regardless of frontiers;

Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,

Have agreed as follows:"

Article 1 – Object and purpose

"The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and

fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").

..."

Article 8 – Additional safeguards for the data subject

"Any person shall be enabled:

a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;

d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with."

Article 9 – Exceptions and restrictions

"1. No exception to the provisions of Articles 5, 6 and 8 of this Convention shall be allowed except within the limits defined in this article.

2. Derogation from the provisions of Articles 5, 6 and 8 of this Convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

b. protecting the data subject or the rights and freedoms of others.

..."

Article 10 – Sanctions and remedies

"Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter."

206. The Explanatory Report explains that:

Article 9 – Exceptions and restrictions

"55. Exceptions to the basic principles for data protection are limited to those which are necessary for the protection of fundamental values in a democratic society. The text of the second paragraph of this article has been modelled after that of the second paragraphs of Articles 6, 8, 10 and 11 of the European Human Rights Convention. It is clear from the decisions of the Commission and the Court of Human Rights relating to the concept of "necessary measures" that the criteria for this concept cannot be laid down for all countries and all times, but should be considered in the light of the given situation in each country.

56. Littera a in paragraph 2 lists the major interests of the State which may require exceptions. These exceptions are very specific in order to avoid that, with regard to the general application of the convention, States would have an unduly wide leeway.

States retain, under Article 16, the possibility to refuse application of the convention in individual cases for important reasons, which include those enumerated in Article 9.

The notion of "State security" should be understood in the traditional sense of protecting national sovereignty against internal or external threats, including the protection of the international relations of the State."

(b) The Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows of 8 November 2001 (CETS No. 181)

207. The Protocol, which has not been ratified by the United Kingdom, provides, insofar as relevant:

Article 1 – Supervisory authorities

"1. Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention and in this Protocol.

2. a. To this end, the said authorities shall have, in particular, powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the principles mentioned in paragraph 1 of Article 1 of this Protocol.

b. Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence.

3. The supervisory authorities shall exercise their functions in complete independence.

4. Decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts.

..."

Article 2 – Transborder flows of personal data to a recipient which is not subject to the jurisdiction of a Party to the Convention

"1. Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer.

2. By way of derogation from paragraph 1 of Article 2 of this Protocol, each Party may allow for the transfer of personal data:

a. if domestic law provides for it because of:

– specific interests of the data subject, or

– legitimate prevailing interests, especially important public interests, or

b. if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law."

(c) Recommendation of the Committee of Ministers on the protection of personal data in the area of telecommunication services

208. This Recommendation (No. R (95) 4 of the Committee of Ministers), which was adopted on 7 February 1995, reads, insofar as relevant, as follows:

"2.4. Interference by public authorities with the content of a communication, including the use of listening or tapping devices or other means of surveillance or interception of communications, must be carried out only when this is provided for by law and constitutes a necessary measure in a democratic society in the interests of:

a. protecting state security, public safety, the monetary interests of the state or the suppression of criminal offences;

b. protecting the data subject or the rights and freedoms of others.

2.5. In the case of interference by public authorities with the content of a communication, domestic law should regulate:

a. the exercise of the data subject's rights of access and rectification;

b. in what circumstances the responsible public authorities are entitled to refuse to provide information to the person concerned, or delay providing it;

c. storage or destruction of such data.

If a network operator or service provider is instructed by a public authority to effect an interference, the data so collected should be communicated only to the body designated in the authorisation for that interference."

(d) The 2001 (Budapest) Convention on Cybercrime

209. The Convention provides, insofar as relevant:

Preamble

"The member States of the Council of Europe and the other States signatory hereto,

...

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

...

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems."

Article 2 – Illegal access

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."

Article 3 – Illegal interception

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system."

Article 4 – Data interference

"1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

..."

Article 15 – Conditions and safeguards

"1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality."

210. The Explanatory Report explains that:

"38. A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self-defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised. Specific examples of such exceptions from criminalisation are provided in relation to specific offences in the corresponding text of the Explanatory Memorandum below. It is left to the Parties to determine how such exemptions are implemented within their domestic legal systems (under criminal law or otherwise).

...

"58. For criminal liability to attach, the illegal interception must be committed "intentionally", and "without right". The act is justified, for example, if the intercepting person has the right to do so, if he acts on the instructions or by authorisation of the participants of the transmission (including authorised testing or protection activities agreed to by the participants), or if surveillance is lawfully authorised in the interests of national security or the detection of offences by investigating authorities."

(e) The 2015 Report of the European Commission for Democracy through Law ("the Venice Commission") on the Democratic Oversight of Signals Intelligence Agencies

211. The Venice Commission noted, at the outset, the value that bulk interception could have for security operations, since it enabled the security services to adopt a proactive approach, looking for hitherto unknown dangers rather than investigating known ones. However, it also noted that intercepting bulk data in transmission, or requirements that telecommunications companies store and then provide telecommunications content data or metadata to law-enforcement or security agencies involved an interference with the privacy and other human rights of a large proportion of the population of the world. In this regard, the Venice Commission considered that the main interference with privacy occurred when stored personal data was accessed and/or processed by the agencies. For this reason, the computer analysis (usually with the help of selectors) was one of the important stages for balancing personal integrity concerns against other interests.

212. According to the report, the two most significant safeguards were the authorisation process (of collection and access) and the oversight process. It was clear from the Court's case-law that the latter must be performed by an independent, external body. While the Court had a preference for judicial authorisation, it had not found this to be a necessary requirement. Rather, the system had to be assessed as a whole, and where independent controls were absent at the authorisation stage, particularly strong safeguards had to exist at the oversight stage. In this regard, the Venice Commission considered the example of the system in the United States, where authorisation was given by the Foreign Intelligence Surveillance Court. However, it noted that despite the existence of judicial authorisation, the lack of independent oversight of the court's conditions was problematic.

213. Similarly, the Commission observed that notification of the subject of surveillance was not an absolute requirement of Article 8 of the Convention. In this regard, a general complaints procedure to an independent oversight body could compensate for non-notification.

214. The report also considered internal controls to be a "primary safeguard". In this regard, recruitment and training were key issues; in addition, it was important for the agencies to build in respect for privacy and other human rights when promulgating internal rules.

215. The report also considered the position of journalists. It accepted that they were a group which required special protection, since searching their contacts could reveal their sources (and the risk of discovery could be a powerful disincentive to whistle-blowers). Nevertheless, it considered there to be no absolute prohibition on searching the contacts of journalists, provided that there were very strong reasons for doing so. It acknowledged,

however, that the journalistic profession was not one which was easily identified, since NGOs were also engaged in building public opinion and even bloggers could claim to be entitled to equivalent protections.

216. Finally, the report briefly considered the issue of intelligence sharing, and in particular the risk that States could thereby circumvent stronger domestic surveillance procedures and/or any legal limits which their agencies might be subject to as regards domestic intelligence operations. It considered that a suitable safeguard would be to provide that the bulk material transferred could only be searched if all the material requirements of a national search were fulfilled and this was duly authorised in the same way as a search of bulk material obtained by the signals intelligence agency using its own techniques.

I. European Union law

1. Charter of Fundamental Rights of the European Union

217. Articles 7, 8 and 11 of the Charter provide as follows:

Article 7 – Respect for private and family life

"Everyone has the right to respect for his or her private and family life, home and communications."

Article 8 – Protection of personal data

"1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which have been collected concerning him or her, and the right to have them rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

Article 11 – Freedom of expression and information

"1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

2. The freedom and pluralism of the media shall be respected."

2. EU directives and regulations relating to protection and processing of personal data

218. The Data Protection Directive (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data), adopted on 24 October 1995, regulated for many years the protection and processing of personal data within the European Union. As the activities of Member States regarding public safety,

defence and State security fall outside the scope of Community law, the Directive did not apply to these activities (Article 3(2)).

219. The General Data Protection Regulation, adopted in April 2016, superseded the Data Protection Directive and became enforceable on 25 May 2018. The regulation, which is directly applicable in Member States[1], contains provisions and requirements pertaining to the processing of personally identifiable information of data subjects inside the European Union, and applies to all enterprises, regardless of location, that are doing business with the European Economic Area. Business processes that handle personal data must be built with data protection by design and by default, meaning that personal data must be stored using pseudonymisation or full anonymisation, and use the highest-possible privacy settings by default, so that the data is not available publicly without explicit consent, and cannot be used to identify a subject without additional information stored separately. No personal data may be processed unless it is done under a lawful basis specified by the regulation, or if the data controller or processor has received explicit, opt-in consent from the data's owner. The data owner has the right to revoke this permission at any time.

220. A processor of personal data must clearly disclose any data collection, declare the lawful basis and purpose for data processing, how long data is being retained, and if it is being shared with any third-parties or outside of the EU. Users have the right to request a portable copy of the data collected by a processor in a common format, and the right to have their data erased under certain circumstances. Public authorities, and businesses whose core activities centre around regular or systematic processing of personal data, are required to employ a data protection officer (DPO), who is responsible for managing compliance with the GDPR. Businesses must report any data breaches within 72 hours if they have an adverse effect on user privacy.

221. The Privacy and Electronic Communications Directive (Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector), adopted on 12 July 2002, states, in recitals 2 and 11:

> "(2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.
>
> (11) Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the

[1] As the United Kingdom is leaving the European Union in 2019, it granted royal assent to the Data Protection Act 2018 on 23 May 2018, which contains equivalent regulations and protections.

measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms."

222. The Directive further provides, insofar as relevant:

Article 1 – Scope and aim

"1. This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law."

Article 15 – Application of certain provisions of Directive 95/46/EC

"1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union."

223. On 15 March 2006 the Data Retention Directive (Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and

amending Directive 2002/58/EC) was adopted. It provided, insofar as relevant:

Article 1 - Subject matter and scope

"1. This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

2. This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network."

Article 3 – Obligation to retain data

"1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned."

3. Relevant case-law of the Court of Justice of the European Union ("CJEU")

(a) *Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources and Others and Seitinger and Others* (Cases C‑293/12 and C-594/12; ECLI:EU:C:2014:238)

224. In a judgment of 8 April 2014 the Court of Justice of the European Union ("the CJEU") declared invalid the Data Retention Directive 2006/24/EC laying down the obligation on the providers of publicly available electronic communication services or of public communications networks to retain all traffic and location data for periods from six months to two years, in order to ensure that the data was available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. The CJEU noted that, even though the directive did not permit the retention of the content of the communication, the traffic and location data covered by it might allow very precise conclusions to be drawn concerning the private lives of the persons whose data had been retained. Accordingly, the obligation to retain the data constituted in itself an interference with the right to respect for private life and communications guaranteed by Article 7 of the Charter of Fundamental Rights of the EU and the right to protection of personal data under Article 8 of the Charter.

225. The access of the competent national authorities to the data constituted a further interference with those fundamental rights, which the CJEU considered to be "particularly serious". The fact that data was retained and subsequently used without the subscriber or registered user being informed was, according to the CJEU, likely to generate in the minds of the persons concerned the feeling that their private lives were the subject of constant surveillance. The interference satisfied an objective of general interest, namely to contribute to the fight against serious crime and terrorism and thus, ultimately, to public security. However, it failed to satisfy the requirement of proportionality.

226. Firstly, the directive covered, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime. It therefore entailed an interference with the fundamental rights of practically the entire European population. It applied even to persons for whom there was no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime.

227. Secondly, the directive did not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. By simply referring, in a general manner, to serious crime, as defined by each Member State in its national law, the directive failed to lay down any objective criterion by which to determine which offences might be considered to be sufficiently serious to justify such an extensive interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. Above all, the access by the competent national authorities to the data retained was not made dependent on a prior review carried out by a court or by an independent administrative body whose decision sought to limit access to the data and their use to what was strictly necessary for the purpose of attaining the objective pursued.

228. Thirdly, the directive required that all data be retained for a period of at least six months, without any distinction being made between the categories of data on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned. The CJEU concluded that the directive entailed a wide-ranging and particularly serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, without such an interference being precisely circumscribed by provisions to ensure that it was actually limited to what was strictly necessary. The CJEU also noted that the directive did not provide for sufficient safeguards, by means of technical and organisational measures, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of those data.

(b) *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* (Cases C-203/15 and C-698/15; ECLI:EU:C:2016:970)

229. In *Secretary of State for the Home Department v. Watson and Others*, the applicants had sought judicial review of the legality of section 1 of the Data Retention and Investigatory Powers Act 2014 ("DRIPA"), pursuant to which the Secretary of State could require a public telecommunications operator to retain relevant communications data if he considered it necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (h) of section 22(2) of RIPA. The applicants claimed, *inter alia*, that section 1 was incompatible with Articles 7 and 8 of the Charter and Article 8 of the Convention.

230. By judgment of 17 July 2015, the High Court held that the *Digital Rights* judgment laid down "mandatory requirements of EU law" applicable to the legislation of Member States on the retention of communications data and access to such data. Since the CJEU, in that judgment, held that Directive 2006/24 was incompatible with the principle of proportionality, national legislation containing the same provisions as that directive could, equally, not be compatible with that principle. In fact, it followed from the underlying logic of the *Digital Rights* judgment that legislation that established a general body of rules for the retention of communications data was in breach of the rights guaranteed in Articles 7 and 8 of the Charter, unless that legislation was complemented by a body of rules for access to the data, defined by national law, which provides sufficient safeguards to protect those rights. Accordingly, section 1 of DRIPA was not compatible with Articles 7 and 8 of the Charter as it did not lay down clear and precise rules providing for access to and use of retained data and access to that data was not made dependent on prior review by a court or an independent administrative body.

231. On appeal by the Secretary of State, the Court of Appeal sought a preliminary ruling from the CJEU.

232. Before the CJEU this case was joined with the request for a preliminary ruling from the Kammarrätten i Stockholm in Case C‑203/15 *Tele2 Sverige AB v Post- och telestyrelsen*. Following an oral hearing in which some fifteen EU Member States intervened, the CJEU gave judgment on 21 December 2016. The CJEU held that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, had to be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, was not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative

authority, and where there is no requirement that the data concerned should be retained within the European Union.

233. The CJEU declared the Court of Appeal's question whether the protection afforded by Articles 7 and 8 of the Charter was wider than that guaranteed by Article 8 of the Convention inadmissible.

234. Following the handing down of the CJEU's judgment, the case was relisted before the Court of Appeal. On 31 January 2018 it granted declaratory relief in the following terms: that section 1 of DRIPA was inconsistent with EU law to the extent that it permitted access to retained data where the object pursued by access was not restricted solely to fighting serious crime; or where access was not subject to prior review by a court or independent administrative authority.

(c) *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service and Secret Intelligence Service* (IPT/15/110/CH; EU OJ C 22, 22.1.2018, p. 29–30)

235. On 8 September 2017 the IPT gave judgment in the case of *Privacy International*, which concerned the acquisition by the agencies of Bulk Communications Data under section 94 of the Telecommunications Act 1984 (a different regime from those which form the subject of the present complaints) and Bulk Personal Data. The IPT found that, following their avowal, the regimes were compliant with Article 8 of the Convention. However, it identified the following four requirements which appeared to flow from the CJEU judgment in *Watson and Others* and which seemed to go beyond the requirements of Article 8 of the Convention: a restriction on non-targeted access to bulk data; a need for prior authorisation (save in cases of validly established emergency) before data could be accessed; provision for subsequent notification of those affected; and the retention of all data within the European Union.

236. On 30 October 2017 the IPT made a request to the CJEU for a preliminary ruling clarifying the extent to which the *Watson* requirements could apply where the bulk acquisition and automated processing techniques were necessary to protect national security. In doing so, it expressed serious concern that if the *Watson* requirements were to apply to measures taken to safeguard national security, they would frustrate them and put the national security of Member States at risk. In particular, it noted the benefits of bulk acquisition in the context of national security (referring to the Bulk Powers Review – see paragraphs 173-176 above); the risk that the need for prior authorisation could undermine the agencies' ability to tackle the threat to national security; the danger and impracticality of implementing a requirement to give notice in respect of the acquisition or use of a bulk database, especially where national security was at stake; and

the impact an absolute bar on the transfer of data outside the European Union could have on Member States' treaty obligations.

THE LAW

I. EXHAUSTION OF DOMESTIC REMEDIES

237. The Government submitted that the applicants in the first and second of the joined cases had not exhausted domestic remedies within the meaning of Article 35 § 1 of the Convention, which provides as follows:

> "1. The Court may only deal with the matter after all domestic remedies have been exhausted, according to the generally recognised rules of international law, and within a period of six months from the date on which the final decision was taken."

A. The parties' submissions

1. The Government

238. The Government argued that the applicants in the first and second of the joined cases had not exhausted domestic remedies as they had failed to raise their complaints before the IPT. The IPT was a bespoke domestic tribunal set up for the very purpose of investigating, considering and ruling on the issues now raised before this Court. In *Kennedy v. the United Kingdom*, no. 26839/05, 18 May 2010 the Court held that the IPT was Article 6 compliant and, as could be seen from the *Liberty* proceedings, it was capable of providing redress. Furthermore, it was advantageous for the Court to have the benefit of a detailed assessment of the operation of the relevant domestic legal regime by a bespoke domestic tribunal with an understanding of that system. That was especially so where, as in the case at hand, domestic law was not only complex, but also involved an assessment of issues of necessity and proportionality which would be particularly difficult to undertake without a proper determination at national level of facts material to the balance between the rights of the individual and the interests of the community as a whole.

239. As for the effectiveness of the IPT as a domestic remedy, the Government noted that it was "one of the most far-reaching systems of judicial oversight over intelligence matters in the world", with broad jurisdiction and remedial powers. It produced open judgments to the extent that it could do so consistently with the public interest. It could investigate and consider in closed session any sensitive material that was relevant to the complaints and produce decisions having regard to that material. On account of its ability to assess and evaluate the adequacy of the internal safeguards, it was in a "special position" to make a proper assessment of

proportionality. In the present case, the applicants' complaints under Articles 8 and 10 of the Convention focussed on the alleged lack of publicly available safeguards and proportionality, and the IPT had the jurisdiction and requisite powers to deal with all of those complaints. It could make clear the extent to which the relevant domestic regime was compatible with the Convention and, if it was not compatible, it could identify the respects in which it was deficient. If there was a lack of foreseeability, it could identify with precision the respects in which the applicable safeguards were not – but should be – public, which, in turn, meant that those aspects of the regime could be remedied by the Government with further disclosure and/or amendments to the Code of Practice. Finally, where proportionality was in issue, it could, through its ability to consider relevant intelligence material in closed proceedings, provide an effective remedy by ordering the quashing of section 8(4) warrants and ordering the destruction of data.

240. Finally, in relation to the IPT's more general declaratory jurisdiction, the Government argued that there was no deficit in Convention terms. On the contrary, it could and did rule on the general lawfulness of regimes about which complaints were made and if it concluded that a regime was contrary to the Convention, it would so state. Furthermore, the Government's reaction to such findings had been consistent. As could be seen from the response to the *Liberty* and *Belhadj* determinations (see paragraphs 92-94 above), it had ensured that any defects were rectified and dealt with. Therefore, even though it has no jurisdiction to make a Declaration of Incompatibility under section 4 of the Human Rights Act 1998, on the facts a finding of incompatibility would be an effective trigger for the necessary changes to ensure Convention compatibility. In light of both this fact, and the Court's increasing emphasis on subsidiarity, the Government contended that the position had moved on since *Kennedy*, in which the Court did not accept that the IPT had provided the applicant with an effective remedy for his general complaint about the Convention compliance of section 8(1) of RIPA.

2. The applicants

241. The applicants in the first and second of the joined cases submitted that they had done all that was required of them in terms of domestic remedies. While they accepted that they did not file complaints with the IPT before lodging their applications with this Court, they had not done so in reliance on the Court's findings in *Kennedy*; namely, that a claim before the IPT was not necessary in order for a general challenge to be brought against the United Kingdom's domestic framework. Although they accepted that it was always open to the Court to reconsider whether a domestic avenue of complaint provided an effective remedy, it had held that an applicant could only be required to make use of a remedy that had developed since the application was lodged if they could still make use of the remedy and it

would not be unjust to declare the application admissible (*Campbell and Fell v. the United Kingdom*, 28 June 1984, §§ 62-63, Series A no. 80).

242. In any event, the applicants argued that there had been no change of circumstances such as would make the IPT an effective remedy. In particular, they relied upon the arguments made by the applicants in the third of the joined cases in support of their Article 6 complaint, and further noted that the IPT could not make a Declaration of Incompatibility. The latter in any case did not constitute an effective remedy, since it did not result in the invalidation of the impugned legislation).

B. The submissions of the third party

243. In its third party intervention, the European Network of National Human Rights Institutions ("ENNHRI") submitted that the international legal framework, including the International Covenant on Civil and Political Rights ("ICCPR") and the American Convention on Human Rights ("ACHR"), and case-law supported the contention that domestic remedies did not have to be followed if they were not capable of providing an effective remedy.

C. The Court's assessment

1. General principles

244. It is a fundamental feature of the machinery of protection established by the Convention that it is subsidiary to the national systems safeguarding human rights. This Court is concerned with the supervision of the implementation by Contracting States of their obligations under the Convention. It should not take on the role of Contracting States, whose responsibility it is to ensure that the fundamental rights and freedoms enshrined therein are respected and protected on a domestic level (*Vučković and Others v. Serbia* (preliminary objection) [GC], nos. 17153/11 and 29 others, § 69, 25 March 2014). However, the application of the rule must make due allowance for the fact that it is being applied in the context of machinery for the protection of human rights that the Contracting Parties have agreed to set up and it must therefore be applied with some degree of flexibility and without excessive formalism (see *Vučković and Others*, cited above, § 76; see also *Akdivar and Others v. Turkey*, 16 September 1996, § 69, *Reports of Judgments and Decisions* 1996-IV and *Gough v. the United Kingdom*, no. 49327/11, § 140, 28 October 2014).

245. States are dispensed from answering before an international body for their acts before they have had an opportunity to put matters right through their own legal system, and those who wish to invoke the supervisory jurisdiction of the Court as concerns complaints against a State

are thus obliged to use first the remedies provided by the national legal system (see, among many authorities, *Vučković and Others*, cited above, § 70 and *Akdivar and Others*, cited above, § 65). The Court is not a court of first instance; it does not have the capacity, nor is it appropriate to its function as an international court, to adjudicate on cases which require the finding of basic facts, which should, as a matter of principle and effective practice, be the domain of domestic jurisdiction (see *Demopoulos and Others v. Turkey* (dec.) [GC], nos. 46113/99, 3843/02, 13751/02, 13466/03, 10200/04, 14163/04, 19993/04 and 21819/04, § 69, ECHR 2010). Similarly, in cases requiring the balancing of conflicting interests under Articles 8 and 10 of the Convention it is particularly important that the domestic courts are first given the opportunity to strike the "complex and delicate" balance between the competing interests at stake. Those courts are in principle better placed than this Court to make such an assessment and, as a consequence, their conclusions will be central to its own consideration of the issue (*MGN Limited v. the United Kingdom*, no. 39401/04, §§ 140-155, 18 January 2011; *Palomo Sánchez and Others v. Spain* [GC], nos. 28955/06, 28957/06, 28959/06 and 28964/06, § 57, 12 September 2011; *Axel Springer AG v. Germany* [GC], no. 39954/08, §§ 85-88, 7 February 2012; *Courtney v. Ireland* (dec), no. 69558/10, 18 December 2012; and *Charron and Merle-Montet v. France* (dec), no. 22612/15, § 30, 16 January 2018).

246. The obligation to exhaust domestic remedies therefore requires an applicant to make normal use of remedies which are available and sufficient in respect of his or her Convention grievances. The existence of the remedies in question must be sufficiently certain not only in theory but in practice, failing which they will lack the requisite accessibility and effectiveness (see *Vučković and Others*, cited above, § 71 and *Akdivar and Others*, cited above, § 66).

247. There is, however, no obligation to have recourse to remedies which are inadequate or ineffective. To be effective, a remedy must be capable of remedying directly the impugned state of affairs and must offer reasonable prospects of success (see *Vučković and Others*, cited above, § 73 and *Sejdovic v. Italy* [GC], no. 56581/00, § 46, ECHR 2006‑II). The existence of mere doubts as to the prospects of success of a particular remedy which is not obviously futile is not a valid reason for failing to exhaust that avenue of redress (see *Vučković and Others*, cited above, § 74 and *Scoppola v. Italy (no. 2)* [GC], no. 10249/03, § 70, 17 September 2009).

248. As regards the burden of proof, it is incumbent on the Government claiming non-exhaustion to satisfy the Court that the remedy was an effective one, available in theory and in practice at the relevant time. Once this burden has been satisfied, it falls to the applicant to establish that the remedy advanced by the Government was in fact exhausted, or was for some reason inadequate and ineffective in the particular circumstances of

the case, or that there existed special circumstances absolving him or her from this requirement (see *Vučković and Others*, cited above, § 77; *McFarlane v. Ireland* [GC], no. 31333/06, § 107, 10 September 2010; *Demopoulos and Others*, cited above, § 69; and *Akdivar and Others*, cited above, § 68).

249. Where an applicant is challenging the general legal framework for secret surveillance measures, the Court has identified the availability of an effective domestic remedy as a relevant factor in determining whether that applicant was a "victim" of the alleged violation, since, in the absence of such a remedy, widespread suspicion and concern among the general public that secret surveillance powers were being abused might be justified (*Roman Zakharov v. Russia* [GC], no. 47143/06, § 171, ECHR 2015).

2. Application of those principles to the case at hand

250. The IPT is a specialist tribunal with sole jurisdiction to hear allegations of wrongful interference with communications as a result of conduct covered by RIPA (see paragraph 124 above). The Court of Appeal has recently observed that the IPT is "a judicial body of like standing and authority to the High Court" and that "[t]he quality of the membership of the IPT in terms of judicial expertise and independence is very high" (see paragraph 135 above). Its members must hold or have held high judicial office or be a qualified lawyer of at least ten years' standing (see paragraph 123 above), and in the present case it was composed of two High Court Judges (including the President), a Circuit Judge and two senior barristers (see paragraph 24 above). It has jurisdiction to investigate any complaint that a person's communications have been intercepted (see paragraph 124 above). In conducting such an investigation, the IPT will generally proceed on the assumption that the facts asserted by the applicant are true and then, acting upon that assumption, decide whether they would constitute lawful or unlawful conduct. In doing so, the IPT considers both the generic compliance of the relevant interception regime (on the basis of assuming there to have been an interception as alleged) as well as, at a subsequent stage, the specific question whether the individual applicant's rights have, in fact, been breached. Those involved in the authorisation and execution of an intercept warrant are required to disclose to the IPT all the documents it may require, including "below the waterline" documents which could not be made public for reasons of national security (see paragraph 127 above), irrespective of whether those documents support or undermine their defence. The IPT has discretion to hold oral hearings, in public, where possible (see paragraphs 131, 138 and 139 above) and, in closed proceedings it may appoint Counsel to the Tribunal to make submissions on behalf of claimants who cannot be represented (see paragraph 142 above). When it determines a complaint the IPT has the power to award compensation and make any other order it sees fit, including

quashing or cancelling any warrant and requiring the destruction of any records (see paragraph 128 above). In considering the complaint brought by the applicants in the third of the joined cases ("the *Liberty* proceedings"), the IPT used all of these powers for the benefit of the applicants.

251. The Court considered the role of the IPT in secret surveillance cases in *Kennedy* (cited above), decided in 2010. In that case the applicant complained that his communications had been intercepted pursuant to a targeted warrant authorised under section 8(1) of RIPA (the specific complaint), and that the targeted interception regime under section 8(1) was not compliant with Article 8 of the Convention (the general compliance complaint). The Court held that the proceedings before the IPT had been Article 6 compliant, since any procedural restrictions were proportionate to the need to keep secret sensitive and confidential information and did not impair the very essence of the applicant's right to a fair trial. With regard to the IPT's effectiveness as a remedy, it acknowledged that Article 35 § 1 had "a special significance in the context of secret surveillance given the extensive powers of the IPT to investigate complaints before it and to access confidential information". It considered these extensive powers to be relevant to the applicant's specific complaint as it had required a factual investigation into whether his communications had been intercepted. However, it was not persuaded of their relevance to the general compliance complaint, since it was a legal challenge and, having already decided the specific complaint, it was unlikely that the IPT could further elucidate the general operation of the surveillance regime and applicable safeguards, such as would assist the Court in its consideration of the compliance of the regime with the Convention. While it accepted that the IPT could consider a complaint about the general compliance of a surveillance regime with the Convention and, if necessary, make a finding of incompatibility, the Government had not addressed in their submissions how such a finding would benefit the applicant, given that it did not appear to give rise to a binding obligation on the State to remedy the incompatibility.

252. Although in *Kennedy* the Court distinguished between a specific and general complaint, it is clear from its more recent case-law that while the two complaints are indeed distinct, they are nevertheless connected. In *Roman Zakharov* the Court identified the availability of an effective domestic remedy to a person who suspects that he or she was subjected to secret surveillance (in other words, an effective domestic remedy for a specific complaint) as a relevant factor in determining whether that person was a "victim" in respect of a complaint challenging the general legal framework for secret surveillance, since, in the absence of such a remedy, widespread suspicion and concern among the general public that secret surveillance powers were being abused might be justified (*Roman Zakharov*, cited above, § 171). In view of the significance the Court has attached to the existence of such a domestic remedy, it would be

problematic if applicants were not required to use it before making either a specific or general complaint to this Court. The Court should not have to consider a challenge to a legislative regime *in abstracto* when the applicants had a domestic forum in which they could have challenged at the very least the possible application of those measures to them.

253. In any event, the IPT's ruling in Mr Kennedy's case came very early in the Tribunal's history. In fact, Mr Kennedy's application, together with an application lodged by British and Irish Rights Watch, was the first time that the IPT sat in public. It was in the context of those applications that it gave its defining ruling on preliminary issues of law and established its current practice (see paragraphs 136-141 above). For the reasons set out below, the Court considers that in view both of the manner in which the IPT has exercised its powers in the fifteen years that have elapsed since that ruling, and the very real impact its judgments have had on domestic law and practice, the concerns expressed by the Court in *Kennedy* about its effectiveness as a remedy for complaints about the general compliance of a secret surveillance regime are no longer valid.

254. First, in *Kennedy* the IPT had fully examined Mr Kennedy's specific complaint about the interception of his communications. The Court was solely concerned with whether an examination of the general complaint could have provided additional clarification. Unlike the present case, therefore, the Court was not being called upon to consider the general complaint entirely *in abstracto*.

255. Secondly, an examination of the IPT's extensive post-*Kennedy* case-law demonstrates the important role that it can and does play in analysing and elucidating the general operation of secret surveillance regimes. For example, in *B v. the Security Services*, Case No IPT/03/01/CH, 21 March 2004 the IPT considered, as a preliminary issue of law, whether the Secretary of State's "neither confirm nor deny" policy was compatible with Article 8 of the Convention. Similarly, in *A Complaint of Surveillance*, Case No IPT/A1/2013, 24 July 2013 the IPT provided elucidation on the meaning of the term "surveillance" in Part II of RIPA. Moreover, given the "secret" nature of most surveillance regimes, the scope of their operation will not always be evident from the "above the waterline" material. For example, in the *Liberty* proceedings the IPT played a crucial role first in identifying those aspects of the surveillance regimes which could and should be further elucidated, and then recommending the disclosure of certain "below the waterline" arrangements in order to achieve this goal. It could therefore be said that the IPT, as the only tribunal with jurisdiction to obtain and review "below the waterline" material, is not only the sole body capable of elucidating the general operation of a surveillance regime; it is also the sole body capable of determining whether that regime requires further elucidation.

256. This "elucidatory" role is of invaluable assistance to the Court when it is considering the compliance of a secret surveillance regime with the Convention. The Court has repeatedly stated that it is not its role to determine questions of fact or to interpret domestic law. That is especially so where domestic law is complex and, for reasons of national security, the State is not at liberty to disclose relevant information to it. Given the confidential nature of the relevant documentation, were applicants to lodge complaints about secret surveillance with this Court without first raising them before the IPT, this Court would either have to become the primary fact-finder in such cases, or it would have to assess necessity and proportionality in a factual vacuum. This difficulty is particularly apparent in respect of those complaints not considered by the IPT in the *Liberty* proceedings; in particular, the Chapter II complaint and the complaint about the receipt of non-intercept material from foreign intelligence services. The Court has before it very limited information about the scope and operation of these regimes and it could therefore only consider these complaints if it were either to accept the applicants' allegations as fact, or to attempt to conduct its own fact-finding exercise. In such cases, therefore, it is particularly important that the domestic courts, which have access to the confidential documentation, first strike the "complex and delicate balance" between the competing interests at stake (see paragraph 245 above).

257. Consequently, on the basis of the information submitted to it, the Court considers that the IPT can – and regularly does – elucidate the general operation of surveillance regimes, including in cases where such elucidation is considered necessary to ensure the regime's Convention compliance.

258. Furthermore, from the information submitted in the present case it would appear that where the IPT has found a surveillance regime to be incompatible with the Convention, the Government have ensured that any defects are rectified and dealt with. In the *Liberty* proceedings, once the IPT had identified which of the "below the waterline" arrangements could and should be made public in order for the intelligence sharing regime to be Convention compliant, the Government agreed to the proposed disclosure ("the 9 October disclosure") and the disclosed material was subsequently added to the amended Code of Practice (see paragraphs 26-30 above). In addition, having found that there had been a breach of Article 8 of the Convention by virtue of the fact that email communications of Amnesty International, which had been intercepted and accessed "lawfully and proportionately", had nevertheless been retained for longer than was permitted under GCHQ's internal policies, the IPT ordered GCHQ to destroy the communications within seven days, and to provide a closed report within fourteen days confirming their destruction (see paragraph 54 above).

259. Similarly, in the *Belhadj* case the Government conceded that from January 2010 the regime for the interception, obtaining, analysis, use,

disclosure and destruction of legally privileged material had not been in accordance with the law for the purposes of Article 8 § 2 of the Convention and was accordingly unlawful. As a consequence, the Security Service and GCHQ confirmed that they would work in the forthcoming weeks to review their policies and procedures (see paragraph 93 above).

260. In addition, in *News Group and Others v. The Commissioner of Police of the Metropolis* the IPT found that the regime under Chapter II of RIPA (for the acquisition of communications data) did not contain effective safeguards to protect Article 10 rights. Although the IPT could not award any remedy in respect of the failure to provide adequate safeguards, as this did not in itself render the authorisations for the acquisition of communications data unlawful, in March 2015 the 2007 ACD Code of Practice was replaced by a new code with enhanced safeguards in respect of applications for communications data designed to identify a journalist's source (see paragraphs 118-120 above). The applicants in that case subsequently lodged a complaint under Article 10 of the Convention with this Court; however, in a recent decision the Court declared the complaint inadmissible as it found that the applicants had not suffered a "significant disadvantage" within the meaning of Article 35 § 3 (b) of the Convention (see *Anthony France and Others v. the United Kingdom* (dec.), nos. 25357/16, 25514/16, 25552/16 and 25597/16, 26 September 2016). In particular, the Court observed that "the applicants have benefitted from a thorough and comprehensive judgment from the IPT, which clearly sets out all the aspects of the interference with their rights". Furthermore, although "the IPT could not find that there had been a violation of their rights, it nonetheless made a clear statement that their rights had been infringed" and a change in the law subsequently occurred (see *Anthony France and Others*, cited above, §§ 43-46).

261. Finally, to cite an earlier example, in *Paton and Others v. Poole Borough Council*, Case Nos IPT/09/01/C, IPT/09/02/C, IPT/09/03/C, IPT/09/04/C and IPT/09/05/C, 29 July 2010, the IPT found that surveillance carried out by a local authority was both unlawful and in breach of Article 8 of the Convention as it was not for the permitted purpose and was neither necessary nor proportionate. While the IPT made no findings regarding the Convention compliance of the regime as a whole, the case was highly publicised and fed into a general public debate about the surveillance powers of local councils. Very shortly after the judgment was handed down, the Government announced that there was to be a review of RIPA which would cover its use by local authorities. Two years later RIPA was amended to restrict the power of local authorities to conduct surveillance.

262. Therefore, while the evidence submitted by the Government may not yet demonstrate the existence of a "binding obligation" requiring it to remedy any incompatibility identified by the IPT, in light of the IPT's "special significance" in secret surveillance cases which arises from its

"extensive powers ... to investigate complaints before it and to access confidential information" (see *Kennedy*, cited above, § 110) the Court would nevertheless accept that the practice of giving effect to its findings on the incompatibility of domestic law with the Convention is sufficiently certain for it to be satisfied as to the effectiveness of the remedy.

263. The effectiveness of the IPT is further underlined by the fact that it can, as a matter of EU law, make an order for reference to the CJEU where an issue arises that is relevant to the dispute before it (see *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service and Secret Intelligence Service*, at paragraph 236 above). The Court has held that the protection of fundamental rights by Community law can be considered to be "equivalent" to that of the Convention system (see *Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi v. Ireland* [GC], no. 45036/98, § 165 ECHR 2005-VI) and it would therefore be surprising if applicants were permitted to bypass a court or tribunal which could have such a significant role in the enforcement of Community law and its fundamental rights guarantees.

264. Insofar as the applicants rely on the fact that the IPT cannot issue a Declaration of Incompatibility (see paragraph 242 above), it is sufficient to note that the Court has not yet accepted that the practice of giving effect to the national courts' Declarations of Incompatibility by amendment of legislation is "so certain as to indicate that section 4 of the Human Rights Act is to be interpreted as imposing a binding obligation" (see *Burden v. the United Kingdom* [GC], no. 13378/05, § 43, ECHR 2008). Consequently, the relevant question is not whether the IPT can issue a Declaration of Incompatibility, but whether the practice of giving effect to its findings is sufficiently certain.

265. In light of the foregoing considerations, the Court finds that as a general rule the IPT has shown itself to be a remedy, available in theory and practice, which is capable of offering redress to applicants complaining of both specific incidences of surveillance and the general Convention compliance of surveillance regimes. As a result, the complaints made by the applicants in the first and second of the joined cases must be declared inadmissible for non-exhaustion unless they can show that there existed special circumstances absolving them from the requirement to exhaust this remedy.

266. In this regard, they contend that precisely such circumstances existed; namely, that at the time they lodged their applications with this Court they were entitled to rely on *Kennedy* as authority for the proposition that the IPT was not an effective remedy for a complaint about the general Convention compliance of a surveillance regime.

267. Although, at first glance, there would appear to be significant differences between the present case and that of *Kennedy* (for example, as the applicant in *Kennedy* had brought a specific complaint to the IPT the Court was not required to consider the more general complaint entirely in the abstract, and in *Kennedy* the applicant's challenge to the RIPA provisions was a challenge to primary legislation as opposed to the whole legal framework governing the relevant surveillance regime), the Government, for their part, have not sought to distinguish *Kennedy* from the case at hand. Moreover, the case-law of the IPT which the Government have relied on as evidence of its effectiveness as a remedy post-dates the introduction before this Court – on 4 September 2013 and 11 September 2014 – of the complaints made by the applicants in the first and second of the joined cases. For example, the main judgment in the *Liberty* proceedings was delivered on 5 December 2014, the *Belhadj* proceedings concluded on 26 February 2015 and *News Group and Others* was decided on 17 December 2015). While the Court has identified some earlier cases which illustrate the effectiveness of the IPT (for example, *B*, *A Complaint of Surveillance* and *Paton and Others*), none of these cases concerned a general complaint about the Convention compliance of a surveillance regime. In comparison, the *Liberty* proceedings, *Belhadj* and *News Group and Others* all demonstrate the important and unique role of the IPT in both elucidating the operation of such regimes, and remedying any breaches of the Convention.

268. Consequently, while the Court acknowledges that since *Kennedy* was decided in 2010 the IPT has shown itself to be an effective remedy which applicants complaining about the actions of the intelligence services and/or the general operation of surveillance regimes should first exhaust in order to satisfy the requirements of Article 35 § 1 of the Convention, it would nevertheless accept that at the time the applicants in the first and second of the joined cases introduced their applications, they could not be faulted for relying on *Kennedy* as authority for the proposition that the IPT was not an effective remedy for a complaint about the general Convention compliance of a surveillance regime. It therefore finds that there existed special circumstances absolving these applicants from the requirement that they first bring their complaints to the IPT and, as a consequence, it considers that their complaints cannot be declared inadmissible pursuant to Article 35 § 1 of the Convention.

II. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

269. Cumulatively, the applicants in the three joined cases complain about the Article 8 compatibility of three discrete regimes: the regime for the bulk interception of communications under section 8(4) of RIPA; the intelligence sharing regime; and the regime for the acquisition of

communications data under Chapter II of RIPA. The Court will consider each of these regimes separately.

A. The section 8(4) regime

270. The applicants in all of the joined cases complain that the regime under section 8(4) of RIPA for the bulk interception of communications is incompatible with their right to respect for their rights under Article 8 of the Convention, which reads as follows:

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

271. The Government contested that argument. They did not, however, raise any objection under Article 1 of the Convention; nor did they suggest that the interception of communications under the section 8(4) regime was taking place outside the United Kingdom's territorial jurisdiction. The Court will therefore proceed on the assumption that the matters complained of fall within the jurisdictional competence of the United Kingdom.

1. Admissibility

272. The Court notes that this complaint is not manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention. It further notes that it is not inadmissible on any other grounds. It must therefore be declared admissible.

2. Merits

(a) The parties' submissions

(i) The applicants

273. The applicants accepted that the bulk interception regime had a basis in domestic law. However, they argued that it lacked the quality of law because it was so complex as to be inaccessible to the public and to the Government, reliance was placed on arrangements which were substantially "below the waterline" rather than on clear and binding legal guidelines, and it lacked sufficient guarantees against abuse.

274. In particular, the applicants submitted that the section 8(4) regime did not comply with the six requirements identified by this Court in *Weber and Saravia v. Germany* (dec.), no. 54934/00, ECHR 2006‑XI. Firstly, they contended that the purposes for which interception could be permitted (such

as "the interests of national security" and "the economic well-being of the United Kingdom) were too vague to provide a clear limit on the intelligence services' activities.

275. Secondly, they argued that in practice any person was liable to have his or her communications intercepted under section 8(4). Although the regime was targeted at "external" communications, there was no clear definition of "internal" and "external" communications, and in any event modern technological developments had rendered the distinction between the two meaningless. While the Secretary of State was required to provide descriptions of the material he considered it necessary to examine, the ISC had reported that section 8(4) warrants were framed in generic terms.

276. Thirdly, with regard to the limits on the duration of surveillance, the applicants submitted that, in practice, a section 8(4) warrant could continue indefinitely, being renewed every six months by the Secretary of State pursuant to section 9(1)(b) of RIPA.

277. Fourthly, according to the applicants the procedure for filtering, storing and analysing intercepted material lacked adequate safeguards and gave rise to an unacceptable risk of an arbitrary and disproportionate interference with Article 8 of the Convention. First of all, there was no requirement that the selectors used to filter intercepted communications be identified in the Secretary of State's certificate accompanying the section 8(4) warrant, and these selectors were not otherwise subject to oversight. Secondly, the section 16 safeguards only applied where a person was "known to be for the time being in the British Islands". Thirdly, the protections in section 16 of RIPA only applied to the "content" of intercepted communications, and not the filtering, storage and analysis of "related communications data", despite the fact that communications data was capable of providing the Government with a detailed profile of the most intimate aspects of a person's private life.

278. Fifthly, in relation to the communication of intercepted material, the applicants contended that the requirement that the Secretary of State ensure that its disclosure was limited to "the minimum that is necessary for the authorised purposes" was an ineffective safeguard. The authorised purposes enumerated in section 15(4) of RIPA were extremely wide, and included situations where the information was or was "likely to become" necessary for any of the purposes specified in section 5(3) of RIPA.

279. Sixth and finally, the applicants submitted that there were no effective or binding safeguards against the disproportionate retention of intercepted data. Indeed, according to the applicants it was clear from the third IPT judgment in the *Liberty* proceedings that Amnesty International's communications had been stored without the appropriate (automated) deletion procedures being followed, and neither the intelligence services nor the oversight and audit mechanisms had detected this.

280. In addition to arguing that the *Webe*r requirements were not satisfied, the applicants in any event contended that they were no longer sufficient to ensure that a communications surveillance regime was compatible with Article 8 of the Convention. *Weber* had been decided in 2006, and subsequent technological developments meant that Governments could now create detailed and intrusive profiles of intimate aspects of private lives by analysing patterns of communications on a bulk basis. The applicants therefore identified a number of additional requirements which they believed were now necessary to ensure the Convention compliance of a legal framework for surveillance: the requirement for objective evidence of reasonable suspicion in relation to the persons for whom data was being sought; prior independent judicial authorisation of interception warrants; and the subsequent notification of the surveillance subject.

281. Finally, the applicants submitted that the section 8(4) regime was disproportionate. In their view the intelligence services were systematically collecting both content and communications data on a massive scale and retaining it for future searching and use. Such a blanket approach fell foul of the principles established in *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, ECHR 2008 and *M.K. v. France*, no. 19522/09, 18 April 2013.

(ii) The Government

282. At the outset, the Government submitted that the information and intelligence obtained under the section 8(4) regime was critical to the protection of the United Kingdom from national security threats; in particular, but not exclusively, from the threat of terrorism. This was especially so given the current level of sophistication of terrorists and criminals in communicating over the Internet in ways that avoided detection, whether through the use of encryption, the adoption of bespoke communications systems, or simply because of the volume of Internet traffic in which they could now hide their communications. Imposing additional fetters on the interception of communications would damage the State's ability to safeguard national security and combat serious crime at exactly the point when advances in communication technology had increased the threat from terrorists and criminals using the Internet.

283. The seriousness of the terrorist threat was underscored by a number of recent attacks across the United Kingdom and Europe, including the attack on Westminster Bridge on 22 March 2017, the Manchester Arena bombing of 22 May 2017, the attack on London Bridge on 3 June 2017, the attacks in Barcelona and Cambrils on 17 August 2017, and the attack on the London Underground on 15 September 2017. The Government therefore submitted that under the Convention scheme, it was properly for States to judge what was necessary to protect the general community from such threats. While those systems were subject to the Court's scrutiny, it had

consistently – and rightly – afforded States a broad margin of appreciation in this field so as not to undermine the effectiveness of systems for obtaining life-saving intelligence that could not be gathered any other way.

284. Although the Government denied that the section 8(4) regime permitted mass surveillance or generalised access to communications, it accepted that it permitted, pursuant to the lawful authority of warrants, the bulk interception of bearers for wanted external communications. In the Government's opinion, the distinction between "internal" and "external" communications was sufficiently clear, and in any event it operated primarily as a safeguard at the macro level; that is, in determining which bearers should be targeted for interception. The Government further contended that bulk interception was critical for the discovery of threats and hitherto unknown targets which might be responsible for threats. Even when the identity of targets was known, they were likely to use a variety of different means of communication, and change those means frequently. Electronic communications did not traverse the Internet by routes that could necessarily be predicted; rather, they took the most efficient route, determined by factors such as cost and the volume of traffic passing over particular parts of the Internet at different times of the day. In addition, communications sent over the Internet were broken down into small pieces (or "packets"), which were transmitted separately, often through different routes. In the opinion of the Government, it was therefore necessary to intercept all communications travelling over more than one bearer to maximise the chance of identifying and obtaining the communications being sent to known targets.

285. With regard to whether the interference complained of was "in accordance with the law", the Government relied on the fact that it had its basis in primary legislation, namely section 8(4) of RIPA, supplemented by the Interception of Communications Code of Practice ("the IC Code"). It had been further clarified by the reports of the Interception of Communications Commissioner, which were also public documents.

286. In relation to the *Weber* requirements the Government argued that the first foreseeability requirement, being the "offences" which might give rise to an interception order, was satisfied by section 5 of RIPA, which defined the purposes for which the Secretary of State could issue an interception warrant. In *Kennedy*, despite the applicant's criticism of the terms "national security" and "serious crime", the Court had found the description of the offences which might give rise to an interception order to be sufficiently clear (*Kennedy*, cited above, § 159).

287. Relying on *Weber*, the Government submitted that the second foreseeability requirement (the categories of people liable to have their communications intercepted) applied at both the interception stage and the selection stage. As regards the interception stage, a section 8(4) warrant was targeted at "external" communications, although in principle it might

authorise the interception of "internal" communications insofar as that was necessary in order to intercept the external communications to which the warrant related. With regard to the selection stage, section 16(1) of RIPA provided that no intercepted material could be read, looked at or listened to by any person unless it fell within the Secretary of State's certificate, and it was proportionate in the circumstances to do so. Furthermore, section 16(2) placed sufficiently precise limits on the extent to which intercepted material could be selected to be read, looked at or listened to according to a factor which was referable to an individual known to be for the time being in the British Islands and which had as (one of) its purpose(s) the identification of material contained in communications sent by or intended for him.

288. The Government further argued that paragraphs 6.22-6.24 of the IC Code made sufficient provision for the duration and renewal of a section 8(4) warrant, thereby complying with the third requirement identified in *Weber*. Pursuant to section 9(2) of RIPA, a section 8(4) warrant could only be renewed if the Secretary of State believed that it continued to be necessary, and if the Secretary of State believed that the warrant was no longer necessary, section 9(3) of RIPA required that it be cancelled.

289. According to the Government, insofar as intercepted material could not be read, looked at or listened to by a person pursuant to section 16 of RIPA, it could not be used at all. Prior to its destruction, paragraph 7.7 of the IC Code required that it be stored securely. For material that could be read, looked at and listened to pursuant to section 16, the Government submitted that the regime satisfied the fourth of the *Weber* requirements. In particular, material had to be selected for examination through the application of search terms by equipment operating automatically for that purpose. If an analyst then wished to select material for examination, paragraphs 7.14-7.16 of the IC Code required that he or she create a record setting out why access was required and proportionate, consistent with the applicable certificate, and stating any circumstances likely to give rise to a degree of collateral infringement of privacy, and any measures taken to reduce the extent of that infringement. That record had to be retained for the purpose of subsequent audit. Paragraphs 7.11-7.20 further required that material should only be read, looked at or listened to by authorised persons receiving regular training in the operation of section 16 of RIPA and the requirements of necessity and proportionality. Finally, material could only be used by the intelligence services in accordance with their statutory functions, and only insofar as was proportionate under section 6(1) of the Human Rights Act 1998.

290. The Government further submitted that the section 8(4) regime satisfied the fifth *Weber* requirement. Section 15(2) set out the precautions to be taken when communicating intercepted material to other people. These precautions served to ensure that only so much intercepted material as was "necessary" for the authorised purpose could be disclosed. Paragraphs 7.4

and 7.5 of the IC Code further provided that where intercepted material was to be disclosed to a foreign State, the intelligence services had to take reasonable steps to ensure that the authorities of that State had and would maintain the necessary procedures to safeguard the intercepted material, and to ensure that it was disclosed, copied, distributed and retained only to the minimum extent necessary. It could only be further disclosed to the authorities of a third country if explicitly agreed. Finally, any disclosure would have to satisfy the constraints imposed by sections 1-2 of the Security Services Act 1989, sections 1-4 of the Intelligence Services Act 1994 as read with section 19(3)-(5) of the Counter Terrorism Act 2008 and section 6(1) of the Human Rights Act 1998.

291. With regard to the final *Weber* requirement, the Government contended that section 15(3) of RIPA and paragraphs 7.8-7.9 of the IC Code made sufficient provision for the circumstances in which intercepted material had to be erased or destroyed (including the obligation to review retention at appropriate intervals, and the specification of maximum retention periods which should normally be no longer than two years).

292. Although the Government acknowledged that the safeguards in section 16 of RIPA did not apply to "related communications data", they argued that the covert acquisition of related communications data was less intrusive than the covert acquisition of content and, as such, the Court had never applied the *Weber* requirements to powers to acquire communications data. It was therefore their contention that instead of the list of six specific foreseeability requirements, the test in respect of communications data should be the more general one of whether the law indicated the scope of any discretion and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.

293. According to the Government, the section 8(4) regime satisfied this test as regards the obtaining and use of related communications data. First of all, "related communications data" as defined in sections 20 and 21 of RIPA was not synonymous with "metadata" but was instead a limited subset of metadata. Secondly, the section 8(4) regime was sufficiently clear as to the circumstances in which the intelligence services could obtain related communications data (namely, by the interception of bearers pursuant to a section 8(4) warrant). Once obtained, access to related communications data had to be necessary and proportionate under section 6(1) of the Human Rights Act 1998 and subject to the constraints in sections 1-2 of the Security Services Act and sections 1-4 of the Intelligence Services Act. Storage, handling, use and disclosure of related communications data, including access by a foreign intelligence partner, would be constrained by section 15 of RIPA and paragraphs 7.1-7.10 of the IC Code. Finally, the Government argued that there was good reason for exempting related communications data from the safeguards in section 16; in order for section 16 to work, the

intelligence services needed to be able to assess whether a potential target was "for the time being in the British Islands".

294. Finally, the Government addressed the applicants' proposals for "updating" the *Weber* requirements. They submitted that any requirement of "reasonable suspicion" would largely preclude the operation of bulk interception regimes, despite the fact that the Court had permitted such monitoring in *Weber*. Furthermore, in *Kennedy* (cited above, § 167) the Court clearly held that judicial authorisation could be either *ex ante* or *post facto*. In that case the Court had found that the oversight provided by the Commissioner, the ISC and the IPT had compensated for any lack of prior judicial authorisation. Finally, any requirement to notify a suspect of the use of bulk data tools against him could fundamentally undermine the work of the intelligence services and potentially threaten the lives of covert human intelligence sources close to the suspect. It would also be wholly impractical in the section 8(4) context, since many of the targets would be overseas and their personal details might be unknown or imperfectly known.

(b) The submissions of the third parties

(i) Article 19

295. Article 19 submitted that mass interception powers were by their very nature inherently incapable of being exercised in a proportionate manner and, as such, were inherently incompatible with the requirements of the Convention. Article 19 therefore urged the Court to conclude that only targeted surveillance based on reasonable suspicion and authorised by a judge constituted a legitimate restriction on the right to privacy.

(ii) Access Now

296. Access Now submitted that the mass surveillance at issue in the present case failed to comply with the International Covenant on Civil and Political Rights ("ICCPR") and the International Principles on the Application of Human Rights to Communications Surveillance since the United Kingdom had not demonstrated that such surveillance was strictly necessary or proportionate. They further contended that surveillance programmes should not be considered independently but should instead be viewed in relation to the entirety of a nation's surveillance activities as machine learning, through which mathematical algorithms could draw inferences from collections of data, had increased the invasiveness of big data sets and data mining.

(iii) ENNHRI

297. The ENNHRI also drew the Court's attention to international instruments such as the ICCPR, the American Convention on Human Rights, and the EU Charter of Fundamental Rights. It observed that in 2015

the Human Rights Committee reviewed the State Party report of the United Kingdom of Great Britain and Northern Ireland. It expressed concern that RIPA provided for untargeted warrants for the interception of external communications without affording the same safeguards as applied to internal communications, and it made a number of detailed recommendations, including the creation of sufficiently precise and foreseeable legal provisions, and judicial involvement in the authorisation of such measures.

(iv) The Helsinki Foundation for Human Rights ("HFHR")

298. The HFHR described their experience challenging the surveillance of communications by public authorities in Poland, which culminated in the Constitutional Tribunal finding certain aspects of the relevant legislation to be unconstitutional. The legislation was subsequently amended.

(v) The International Commission of Jurists ("ICJ")

299. The ICJ submitted that in light of the scale and scope of the interference with privacy entailed in mass surveillance, the distinction between the acquisition of metadata and content had become out-dated. Furthermore, the fact that, in a mass surveillance operation, elements of the interference with rights might take place outside a State's territorial jurisdiction didn't preclude that State's responsibility, since its control over the information was sufficient to establish jurisdiction.

(vi) Open Society Justice Initiative ("OSJI")

300. OSJI submitted that both the amount of data available for interception today and governments' appetite for data far exceeded what was possible in the past. Consequently, bulk interception was a particularly serious interference with privacy which could, through its "chilling effect", potentially interfere with other rights such as freedom of expression and freedom of association. To be lawful, bulk interception should therefore satisfy several preconditions: the governing law had to be sufficiently precise; the scope of the information gathered had to be limited by time and geography; and information should only be gathered based on "reasonable suspicion".

(vii) European Digital Rights ("EDRi") and other organisations active in the field of human rights in the information society

301. EDRi and others argued that the present case offered the Court a crucial opportunity to revise its framework for the protection of metadata. Governments had built their surveillance programmes based on the distinction drawn between content and metadata in *Malone v. the United Kingdom*, 2 August 1984, Series A no. 82, but at the time that case was decided neither the Internet nor mobile phones existed. Today, metadata

could paint a detailed and intimate picture of a person: it allowed for mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with. Moreover, the level of detail that could be gleaned was magnified when analysed on a large scale. Indeed, Stewart Baker, general counsel of the NSA, had indicated that metadata could disclose everything about someone's life, and that if you had enough metadata, you wouldn't need content. As a result, different degrees of protection should not be afforded to personal data based on the arbitrary and irrelevant distinction between content and metadata, but rather on the inferences that could be drawn from the data.

(viii) The Law Society of England and Wales

302. The Law Society expressed deep concern about the implications of the section 8(4) regime for the principle of legal professional privilege. In particular, the regime permitted the interception of legally privileged and confidential communications between lawyers and clients, even when both were in the United Kingdom. It also permitted the routine collection of metadata attaching to such communications. Furthermore, once intercepted these legally privileged communications could be used, provided that the primary purpose and object of the warrant was the collection of external communications. This arrangement – and the absence of adequate constraints on the use of such material – was apt to have a potentially severe chilling effect on the frankness and openness of lawyer-client communications.

(c) The Court's assessment

(i) General principles relating to secret measures of surveillance, including the interception of communications

303. Although the Court has developed extensive jurisprudence on secret measures of surveillance, its case-law concerns many different forms of surveillance, including, but not limited to, the interception of communications. It also concerns many different forms of "interference" with applicants' right to respect for their private lives; for example, while some cases concern the interception of the content of communications, others concern the interception or obtaining of communications data, or the tracking of individuals via GPS. As the Court has at times differentiated between the different types of surveillance and the different forms of interference, there is no one set of general principles which apply in all cases concerning secret measures of surveillance. The following principles can, however, be extrapolated from the Court's case-law.

304. Any interference with an individual's Article 8 rights can only be justified under Article 8 § 2 if it is in accordance with the law, pursues one

or more of the legitimate aims to which that paragraph refers and is necessary in a democratic society in order to achieve any such aim (see *Roman Zakharov*, cited above, § 227, and *Kennedy*, cited above, § 130).

305. According to the Court's well established case-law, the wording "in accordance with the law" requires the impugned measure to have some basis in domestic law (as opposed to a practice which does not have a specific legal basis – see *Heglas v. the Czech Republic*, no. 5935/02, § 74, 1 March 2007). It must also be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must therefore be accessible to the person concerned and foreseeable as to its effects (see *Roman Zakharov*, cited above, § 228; see also, among many other authorities, *Rotaru v. Romania* [GC], no. 28341/95, § 52, ECHR 2000‑V; *S. and Marper*, cited above, § 95, and *Kennedy*, cited above, § 151).

306. The Court has held on several occasions that the reference to "foreseeability" in the context of secret surveillance cannot be the same as in many other fields. Foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to resort to such measures so that he can adapt his conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on secret surveillance measures, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (see *Roman Zakharov*, cited above, § 229; see also *Malone*, cited above, § 67, *Leander*, cited above, § 51; *Huvig v. France*, 24 April 1990, § 29, Series A no. 176‑B; *Valenzuela Contreras v. Spain*, 30 July 1998, § 46, Reports of Judgments and Decisions 1998‑V; *Rotaru*, cited above, § 55; *Weber and Saravia*, cited above, § 93; *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, § 75, 28 June 2007). Moreover, the law must indicate the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see *Roman Zakharov*, cited above, § 230; see also, among other authorities, *Malone*, cited above, § 68; *Leander*, cited above, § 51; *Huvig*, cited above, § 29; and *Weber and Saravia*, cited above, § 94).

307. In its case-law on the interception of communications in criminal investigations, the Court has developed the following minimum requirements that should be set out in law in order to avoid abuses of power: the nature of offences which may give rise to an interception order; a

definition of the categories of people liable to have their communications intercepted; a limit on the duration of interception; 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 intercepted data may or must be erased or destroyed (see *Huvig*, cited above, § 34; *Valenzuela Contreras*, cited above, § 46; *Weber and Saravia*, cited above, § 95; and *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 76). In *Roman Zakharov* (cited above, § 231) the Court confirmed that the same six minimum requirements also applied in cases where the interception was for reasons of national security; however, in determining whether the impugned legislation was in breach of Article 8, it also had regard to the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law (*Roman Zakharov*, cited above, § 238).

308. As to the question whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, the Court has acknowledged that, when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. However, this margin is subject to European supervision embracing both legislation and decisions applying it. In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the 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. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" to what is "necessary in a democratic society" (see *Roman Zakharov*, cited above, § 232; see also *Klass and Others v. Germany*, 6 September 1978, §§ 49, 50 and 59, Series A no. 28, *Weber and Saravia*, cited above, § 106 and *Kennedy*, cited above, §§ 153 and 154).

309. Review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will

necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure (see *Roman Zakharov*, cited above, § 233; see also *Klass and Others*, cited above, §§ 55 and 56).

310. As regards the third stage, after the surveillance has been terminated, the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers. There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively (see *Roman Zakharov*, cited above, § 234; see also *Klass and Others*, cited above, § 57, and *Weber and Saravia*, cited above, § 135) or, in the alternative, unless any person who suspects that he or she has been subject to surveillance can apply to courts, whose jurisdiction does not depend on notification to the surveillance subject of the measures taken (see *Roman Zakharov*, cited above, § 234; see also *Kennedy*, cited above, § 167).

(ii) Existing case-law on the bulk interception of communications

311. The Court has considered the Convention compatibility of regimes which expressly permit the bulk interception of communications on two occasions: first in *Weber and Saravia* (cited above), and then in *Liberty and Others v. the United Kingdom*, no. 58243/00, 1 July 2008.

312. In *Weber and Saravia* the applicants complained about the process of strategic monitoring under the amended G10 Act, which authorised the monitoring of international wireless telecommunications. Signals emitted from foreign countries were monitored by interception sites situated on German soil with the aid of certain catchwords which were listed in the monitoring order. Only communications containing these catchwords were recorded and used. Having particular regard to the six "minimum requirements" set out in paragraph 307 above, the Court considered that there existed adequate and effective guarantees against abuses of the State's strategic monitoring powers. It therefore declared the applicants' Article 8 complaints to be manifestly ill-founded.

313. In *Liberty and Others* the Court was considering the regime under section 3(2) of the Interception of Communications Act 1985, which was in effect the predecessor of the regime under section 8(4) of RIPA.

Section 3(2) allowed the executive to intercept communications passing between the United Kingdom and an external receiver. At the time of issuing a section 3(2) warrant, the Secretary of State was required to issue a certificate containing a description of the intercepted material which he considered should be examined. The 1985 Act provided that material could be contained in a certificate, and thus listened to or read, if the Secretary of State considered that this was required in the interests of national security, the prevention of serious crime or the protection of the United Kingdom's economy. However, external communications emanating from a particular address in the United Kingdom could only be included in a certificate for examination if the Secretary of State considered it necessary for the prevention or detection of acts of terrorism. The Court held that the domestic law at the relevant time (which predated the adoption of the Interception of Communications Code of Practice – see, in particular, paragraph 109 above) did not indicate with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. In particular, it did not set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material.

(iii) The test to be applied in the present case

314. The Court has expressly recognised that the national authorities enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security (see *Weber and Saravia*, cited above, § 106). Furthermore, in *Weber and Saravia* and *Liberty and Others* the Court accepted that bulk interception regimes did not *per se* fall outside this margin. Although both of these cases are now more than ten years old, given the reasoning of the Court in those judgments and in view of the current threats facing many Contracting States (including the scourge of global terrorism and other serious crime, such as drug trafficking, human trafficking, the sexual exploitation of children and cybercrime), advancements in technology which have made it easier for terrorists and criminals to evade detection on the Internet, and the unpredictability of the routes via which electronic communications are transmitted, the Court considers that the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States' margin of appreciation.

315. Nevertheless, as indicated previously, it is evident from the Court's case-law over several decades that all interception regimes (both bulk and targeted) have the potential to be abused, especially where the true breadth of the authorities' discretion to intercept cannot be discerned from the relevant legislation (see, for example, *Roman Zakharov*, cited above, and

Szabó and Vissy v. Hungary, no. 37138/14, 12 January 2016). Therefore, while States enjoy a wide margin of appreciation in deciding what type of interception regime is necessary to protect national security, the discretion afforded to them in operating an interception regime must necessarily be narrower. In this regard, the Court has identified six minimum requirements that both bulk interception and other interception regimes must satisfy in order to be sufficiently foreseeable to minimise the risk of abuses of power (see paragraph 307 above).

316. The applicants argue that in the present case the Court should "update" those requirements by including requirements for objective evidence of reasonable suspicion in relation to the persons for whom data is being sought, prior independent judicial authorisation of interception warrants, and the subsequent notification of the surveillance subject (see paragraph 280 above). In their view, such changes would reflect the fact that due to recent technological developments the interception of communications now has greater potential than ever before to paint an intimate and detailed portrait of a person's private life and behaviour. However, while the Court does not doubt the impact of modern technology on the intrusiveness of interception, and has indeed emphasised this point in its case-law, it would be wrong automatically to assume that bulk interception constitutes a greater intrusion into the private life of an individual than targeted interception, which by its very nature is more likely to result in the acquisition and examination of a large volume of his or her communications. In any event, although the Court would agree that the additional requirements proposed by the applicants might constitute important safeguards in some cases, for the reasons set out below it does not consider it appropriate to add them to the list of minimum requirements in the case at hand.

317. First of all, requiring objective evidence of reasonable suspicion in relation to the persons for whom data is being sought and the subsequent notification of the surveillance subject would be inconsistent with the Court's acknowledgment that the operation of a bulk interception regime in principle falls within a State's margin of appreciation. Bulk interception is by definition untargeted, and to require "reasonable suspicion" would render the operation of such a scheme impossible. Similarly, the requirement of "subsequent notification" assumes the existence of clearly defined surveillance targets, which is simply not the case in a bulk interception regime.

318. Judicial authorisation, by contrast, is not inherently incompatible with the effective functioning of bulk interception. Nevertheless, as the Venice Commission acknowledged in their report on the Democratic Oversight of Signals Intelligence Agencies (see paragraph 212 above), while the Court has recognised that judicial authorisation is an "important safeguard against arbitrariness" (see *Roman Zakharov*, cited above, § 249),

to date it has not considered it to be a "necessary requirement" or the exclusion of judicial control to be outside "the limits of what may be deemed necessary in a democratic society" (see, for example, *Roman Zakharov*, cited above, § 258; see also *Klass and Others*, cited above, §§ 51 and 56; *Weber and Saravia*, cited above, § 115; *Kennedy*, cited above, § 167; and *Szabó and Vissy*, cited above, § 77*)*. There would appear to be good reason for this. The Court has found it "desirable to entrust supervisory jurisdiction to a judge" because, as a result of the secret nature of the surveillance, the individual will usually be unable to seek a remedy of his or her own accord (see *Roman Zakharov*, cited above, § 233). However, that is not the case in every contracting State. In the United Kingdom, for example, any person who thinks that he or she has been subject to secret surveillance can lodge a complaint with the IPT (see paragraph 250 above). Consequently, in *Kennedy* the Court accepted that regardless of the absence of prior judicial authorisation, the existence of independent oversight by the IPT and the Interception of Communications Commissioner provided adequate safeguards against abuse (see *Kennedy*, cited above, §§ 167-169). In this regard, the Venice Commission also noted that independent oversight may be able to compensate for an absence of judicial authorisation (see paragraph 212 above).

319. Secondly, the Court has acknowledged that "the possibility of improper action by a dishonest, negligent or over-zealous official can never be completely ruled out whatever the system" (see *Klass and Others*, cited above, § 59), and one need only look at its most recent jurisprudence to find examples of cases where prior judicial authorisation provided limited or no protection against abuse. For example, in *Roman Zakharov*, any interception of communications had to be authorised by a court and the judge had to give reasons for the decision to authorise interceptions. However, as judicial scrutiny was limited in scope and the police had the technical means to circumvent the authorisation procedure and to intercept any communications without obtaining prior judicial authorisation, the Court found that Russian law was incapable of keeping the "interference" to what was "necessary in a democratic society". Similarly, in *Association for European Integration and Human Rights and Ekimdzhiev* the relevant law required judicial authorisation before interception could take place. Nevertheless, the Court found that numerous abuses had taken place (according to a recent report, more than 10,000 warrants were issued over a period of some twenty‑four months). More recently, in *Mustafa Sezgin Tanrıkulu v. Turkey*, no. 27473/06, § 64, 18 July 2017 the Court found a violation of Article 8 where an assize court had granted the National Intelligence Agency permission to intercept all domestic and international communications for a month and a half with a view to identifying terrorist suspects.

320. Therefore, while the Court considers judicial authorisation to be an important safeguard, and perhaps even "best practice", by itself it can neither be necessary nor sufficient to ensure compliance with Article 8 of the Convention (see *Klass and Others*, cited above, § 56). Rather, regard must be had to the actual operation of the system of interception, including the checks and balances on the exercise of power, and the existence or absence of any evidence of actual abuse (see *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 92). Accordingly, the Court will examine the justification for any interference in the present case by reference to the six minimum requirements, adapting them where necessary to reflect the operation of a bulk interception regime. It will also have regard to the additional relevant factors which it identified in *Roman Zakharov*, but did not classify as "minimum requirements"; namely, the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law (see paragraph 307 above).

(α) The existence of an interference

321. The Government do not dispute that there has been an interference with the applicants' Article 8 rights.

(β) Justification for the interference

322. As already noted, an interference can only be justified under Article 8 § 2 if it is in accordance with the law, pursues one or more legitimate aims and is necessary in a democratic society in order to achieve any such aim (see paragraph 303 above). In cases where the legislation permitting secret surveillance is contested before the Court, the lawfulness of the interference is closely related to the question whether the "necessity" test has been complied with and it is therefore appropriate for the Court to address jointly the "in accordance with the law" and "necessity" requirements (see *Roman Zakharov*, cited above, § 236 and *Kennedy*, cited above, § 155). The "quality of law" in this sense implies that the domestic law must not only be accessible and foreseeable in its application, but it must also ensure that secret surveillance measures are applied only when "necessary in a democratic society", in particular by providing for adequate and effective safeguards and guarantees against abuse.

323. The parties do not dispute that the section 8(4) regime had a basis in domestic law; nor do they dispute that the regime pursued the legitimate aims of the protection of national security, the prevention of crime and the protection of the economic well-being of the country. The applicants do, however, contest the quality of domestic law and, in particular, its accessibility and foreseeability.

324. The Court will therefore assess in turn the accessibility of the domestic law, followed by its foreseeability and necessity, having regard to

the six minimum requirements established in its case law, before turning its attention to the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law (see paragraph 307 above).

- *Accessibility*

325. The applicants challenge the accessibility of domestic law on the grounds that it is too complex to be accessible to the public, and it relies on "below the waterline" arrangements. It is true that most of the reports into the United Kingdom's secret surveillance regimes have criticised the piecemeal development – and subsequent lack of clarity – of the legal framework (see paragraphs 152, 162 and 167 above). However, as with other cases in which domestic law has been considered *in abstracto* and amendments have been made to the legislation while the application was pending (see, for example, *Association for European Integration and Human Rights and Ekimdzhiev*), in the present case the Court must review the Convention compliance of the law in force at the date of its examination of the applicants' complaints. It therefore can, and should, take into account the IC Code which was amended in 2016 to clarify the legal framework and reflect the further disclosures which were made following the Snowden revelations and which are examined in detail in the ISC report, the Anderson report and the ISR report (see paragraphs 90, 148-150, 160-165 and 166-172 above). As the IC Code is a public document, subject to the approval of both Houses of Parliament, and has to be taken into account both by those exercising interception duties and by courts and tribunals, the Court has expressly accepted that its provisions could be taken into consideration in assessing the foreseeability of the RIPA regime (see *Kennedy*, cited above, § 157).

326. Insofar as the applicants complain about the existence of "below the waterline" arrangements, the Court has acknowledged that States do not have to make public all the details of the operation of a secret surveillance regime, provided that sufficient information is available in the public domain (see *Roman Zakharov*, cited above, §§ 243-244 and 247; see also, among many examples, *Szabó and Vissy*, cited above, § 64, and *Kennedy*, cited above, § 159). In the context of secret surveillance, it is inevitable that "below the waterline" arrangements will exist, and the real question for the Court is whether it can be satisfied, based on the "above the waterline" material, that the law is sufficiently foreseeable to minimise the risk of abuses of power. This is a question that goes to the foreseeability and necessity of the relevant law, rather than its accessibility.

327. Therefore, while the Court concurs with several of the aforementioned domestic reports that RIPA and the accompanying surveillance framework are extremely complex, in the present case it will concentrate on the requirements of "foreseeability" and "necessity".

- *The scope of application of secret surveillance measures*

328. The first two minimum requirements have traditionally been referred to as the nature of the offences which might give rise to an interception order and a definition of the categories of people liable to have their telephones tapped. In *Roman Zakharov* the Court made clear that pursuant to these two requirements "the national law must define the scope of application of secret surveillance measures by giving citizens an adequate indication as to the circumstances in which public authorities are empowered to resort to such measures" (see *Roman Zakharov*, cited above, §§ 243).

329. In a targeted interception regime, the nature of the communications to be intercepted should be tightly defined, but once interception takes place it is likely that all – or nearly all – of the intercepted communications are analysed. The opposite will normally be true of a bulk interception regime, where the discretion to intercept is broader, but stricter controls will be applied at the selection for examination stage. In fact, in the present case, it is clear from Chapter 6 of the IC Code (see paragraph 90 above), the ISC report (see paragraphs 151-159 above), the first IPT judgment in the *Liberty* proceedings (see paragraphs 41-49 above) and the Government's observations that there are four distinct stages to the section 8(4) regime:

1. The interception of a small percentage of Internet bearers, selected as being those most likely to carry external communications of intelligence value.

2. The filtering and automatic discarding (in near real-time) of a significant percentage of intercepted communications, being the traffic least likely to be of intelligence value.

3. The application of simple and complex search criteria (by computer) to the remaining communications, with those that match the relevant selectors being retained and those that do not being discarded.

4. The examination of some (if not all) of the retained material by an analyst).

330. Thus, in addressing the first two minimum requirements, the Court will examine first, whether the grounds upon which a warrant can be issued are sufficiently clear; secondly, whether domestic law gives citizens an adequate indication of the circumstances in which their communications might be intercepted; and thirdly, whether domestic law gives citizens an adequate indication of the circumstances in which their communications might be selected for examination (see paragraph 328 above).

331. According to RIPA and the IC Code, the Secretary of State can only issue a warrant if he is satisfied that it is necessary in the 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 so far as those interests are also relevant to the interests of national security; and that the conduct authorised by the warrant is

proportionate to what is sought to be achieved by that conduct. Pursuant to domestic law, when assessing necessity and proportionality, account should be taken of whether the information sought under the warrant could reasonably be obtained by other means (section 5(3) of RIPA and Chapter 6 of the IC Code – see paragraphs 57 and 90 above). It is clear that insofar as RIPA and the IC Code use the terms "necessity" and "proportionality" they are intended to ensure compliance with the requirements of Articles 8 and 10 of the Convention and should therefore be understood in the Convention sense (see paragraph 3.5 of the IC Code, at paragraph 90 above).

332. The Court has held that the condition of foreseeability does not require States to set out exhaustively by name the specific offences which may give rise to interception, provided that there is sufficient detail about the nature of the offences in question (see *Roman Zakharov*, cited above, §§ 243-244; see also, among many examples, *Szabó and Vissy*, cited above, § 64, and *Kennedy*, cited above, § 159). Moreover, the Court has expressly recognised the need to avoid excessive rigidity in the wording of certain statures and to keep pace with changing circumstances (see *Szabó and Vissy*, cited above, § 64 and *Kokkinakis v. Greece*, 25 May 1993, § 40, Series A no. 260-A).

333. In *Kennedy* the Court had to consider whether the section 5(3) grounds (which apply to both section 8(1) and section 8(4) warrants) provided sufficient detail about the nature of the offences that might give rise to an interception order. It found that the term "national security" was frequently employed in both national and international legislation and constituted one of the legitimate aims to which Article 8 § 2 referred. It further noted that threats to national security tended to vary in character and might be unanticipated or difficult to define in advance. Finally, the Interception of Communications Commissioner had clarified that in practice "national security" allowed surveillance of activities which threatened the safety or well-being of the State and activities which were intended to undermine or overthrow Parliamentary democracy by political, industrial or violent means. It therefore found the term to be sufficiently clear (see *Kennedy*, cited above, § 159).

334. Furthermore, the Court observes that "serious crime" is clearly defined in section 81 of RIPA (see paragraphs 58-59 above; see also *Kennedy*, cited above, § 159) and the IC Code has clarified that the purpose of safeguarding the economic well-being of the United Kingdom is restricted to those interests which are also relevant to the interests of national security (see paragraph 90 above).

335. The Court therefore considers that section 5(3) is sufficiently clear, giving citizens an adequate indication of the circumstances in which and the conditions on which a section 8(4) warrant might be issued.

336. As for the persons liable to have their communications intercepted, it is clear that this category is wide. Section 8(4) only permits the Secretary

of State to issue a warrant for the interception of external communications, which in principle excludes communications where both of the parties are in the British Islands. Although there has been some confusion about the application of the terms "external communications" and "internal communications" to modern forms of communications, the Secretary of State for the Foreign and Commonwealth, in giving evidence to the Intelligence and Security Committee of Parliament in October 2014, provided clarification about the status of emails, web-browsing, social media and cloud storage (see paragraph 71 above). However, even where it is clear that a communication is "internal", as it is between two people in the British Islands, in practice, some or all of its parts might be routed through one or more other countries, and would therefore be at risk of being intercepted under the section 8(4) regime. This is expressly permitted by section 5(6) of RIPA, which allows the interception of communications not identified in the warrant (see paragraph 63 above).

337. That being said, it is clear that the targeted bearers are not chosen at random. They are selected because they are believed to be the most likely to carry external communications of intelligence interest (paragraph 6.7 of the IC Code, at paragraph 90 above and the Annual Report of the Interception of Communications Commissioner for 2016, at paragraph 178 above). Therefore, while anyone could potentially have their communications intercepted under the section 8(4) regime, it is clear that the intelligence services are neither intercepting everyone's communications, nor exercising an unfettered discretion to intercept whatever communications they wish. In practice, one of the grounds set out in section 5(3) of RIPA must be satisfied, bulk interception must be proportionate to the aim sought to be achieved, and – at least at the macro level of selecting the bearers for interception – only external communications can be targeted.

338. As the ISC observed, it would be desirable for the criteria for selecting the bearers to be subject to greater oversight by the Commissioner (see paragraph 157 above). However, the Court has already noted that by its very nature a bulk interception regime will allow the authorities a broad discretion to intercept communications and, as such, it does not consider this fact alone to be fatal to the Article 8 compliance of the section 8(4) regime. While the discretion to intercept should not be unfettered – since the interception and filtering of a communication, even if it is subsequently discarded in near real-time, is sufficient to constitute an interference with a persons' rights under Article 8 of the Convention –, more rigorous safeguards will be required at the third and fourth stages identified in paragraph 329 above, as any interference in such cases will be significantly greater.

339. With regard to the selection of communications for examination, once communications are intercepted and filtered, those not discarded in near real-time are further searched; in the first instance by the automatic

application, by computer, of simple selectors (such as email addresses or telephone numbers) and initial search criteria, and subsequently by the use of complex searches (see paragraph 6.4 of the IC Code at paragraph 90; see also the ISC report at paragraphs 151-159 above and the Government's observations in the present case). In *Liberty and Others*, the Court compared the predecessor of the section 8(4) regime unfavourably with the German system under consideration in *Weber and Saravia*, noting that the G10 Act authorised the Federal Intelligence Service to carry out monitoring of communications only with the aid of search terms which served, and were suitable for, the investigation of the dangers described in the monitoring order and which search terms had to be listed in the monitoring order (*Liberty and Others*, cited above, § 68 and *Weber and Saravia*, cited above, § 32).

340. This does not mean that selectors and search criteria need to be made public; nor does it mean that they necessarily need to be listed in the warrant ordering interception. In fact, in the *Liberty* proceedings the IPT found that the inclusion of the selectors in the warrant or accompanying certificate would "unnecessarily undermine and limit the operation of the warrant and be in any event entirely unrealistic" (see paragraph 44 above). The Court has no reason to call this conclusion into question. Nevertheless, the search criteria and selectors used to filter intercepted communications should be subject to independent oversight; a safeguard which appears to be absent in the section 8(4) regime. Indeed, the ISC report criticised the absence of any meaningful oversight of both the selectors and search criteria (see paragraph 157 above).

341. As a result of the application of selectors and automated searches, an index is generated. Material not on the index is discarded. Only material on the index may be examined by an analyst, and only if it satisfies the two criteria in section 16 of RIPA, namely certification by the Secretary of State as to necessity (section 16(1); see paragraphs 78-85 above) and presence for the time being in the British Islands (section 16(2)).

342. As regards the certification by the Secretary of State, the ISC observed that the categories set out in the certificates were set out in very general terms (for example, "material providing intelligence on terrorism (as defined by the Terrorism Act 2000 (as amended)) including, but not limited to, terrorist organisations, terrorists, active sympathisers, attack planning, fund-raising") (see paragraph 156 above). Similarly, the Independent Reviewer of Terrorism Legislation recommended that the purposes for which material or data was sought should be spelled out by reference to specific operations or mission purposes (for example, "attack planning by ISIL in Iraq/Syria against the UK") (see paragraph 162 above). In order for this safeguard to be effective, the Court agrees that it would be highly desirable for the certificate to be expressed in more specific terms than it currently appears to be.

343. On the other hand, the exclusion of communications of individuals known currently to be in the British Islands is, in the opinion of the Court, an important safeguard, since persons of interest to the intelligence services who are known to be in the British Islands could be subject to a targeted warrant under section 8(1) of RIPA. The intelligence services should not be permitted to obtain via a bulk warrant what they could obtain via a targeted warrant.

344. According to paragraph 7.18 of the IC Code, periodic audits should be carried out to ensure that the requirements set out in section 16 of RIPA are being met and any breaches of safeguards should be notified to the Interception of Communications Commissioner (see paragraph 90 above). In his 2016 annual report, echoing comments also made in his 2014 and 2015 reports, the Commissioner observed that the process by which analysts selected material for examination, which did not require pre-authorisation by a more senior operational manager, relied mainly on the professional judgment of analysts, their training and subsequent management oversight (see paragraph 179 above).

345. On balance, the Court agrees that it would be preferable for the selection of material by analysts to be subject at the very least to pre-authorisation by a senior operational manager. However, given that analysts are carefully trained and vetted, records are kept and those records are subject to independent oversight and audit (see paragraph 7.15 and 7.18 of the IC Code, at paragraph 90 above), the absence of pre-authorisation would not, in and of itself, amount to a failure to provide adequate safeguards against abuse.

346. Nevertheless, the Court must have regard to the operation of the section 8(4) regime as a whole, and in particular the fact that the list from which analysts are selecting material is itself generated by the application of selectors and selection criteria which were not subject to any independent oversight. In practice, therefore, the only independent oversight of the process of filtering and selecting intercept data for examination is the *post factum* audit by the Interception of Communications Commissioner and, should an application be made to it, the IPT. In *Kennedy* the Court held that the RIPA procedure for examining intercept material was sufficiently clear. That finding, however, was expressly based on the fact that unlike the regime examined in *Liberty and Others*, which concerned the indiscriminate capturing of data, that case was concerned with an interception warrant for one set of premises only; a fact which in and of itself limited the scope of the authorities' discretion to intercept and listen to private communications (see *Kennedy*, cited above, § 162). In a bulk interception regime, where the discretion to intercept is not significantly curtailed by the terms of the warrant, the safeguards applicable at the filtering and selecting for examination stage must necessarily be more robust.

347. Therefore, while there is no evidence to suggest that the intelligence services are abusing their powers – on the contrary, the Interception of Communications Commissioner observed that the selection procedure was carefully and conscientiously undertaken by analysts (see paragraph 179 above) –, the Court is not persuaded that the safeguards governing the selection of bearers for interception and the selection of intercepted material for examination are sufficiently robust to provide adequate guarantees against abuse. Of greatest concern, however, is the absence of robust independent oversight of the selectors and search criteria used to filter intercepted communications.

- The exemption of related communications data from the safeguards applicable to the searching and examining of content

348. The Article 8(4) regime permits the bulk interception of both content and related communications data (the latter being the "who, when and where" of a communication). However, section 16 applies only to "intercepted material" which, according to the interpretation provision in section 20 of RIPA, is defined as the content of intercepted communications (see paragraph 78 above). The related communications data of all intercepted communications – even internal communications incidentally intercepted as a "by-catch" of a section 8(4) warrant – can therefore be searched and selected for examination without restriction.

349. The Government contend that access to communications data is necessary to give effect to one of the section 16 safeguards, namely to determine whether a person is or is not in the British Islands. They further contend that as communications data is less intrusive than data relating to content (at least when compared on a like-for-like basis), its interception, storage and use should not be subject to the same six minimum requirements (see paragraph 307 above). Instead, the Court should simply ask whether the law was sufficiently clear to give the individual adequate protection against arbitrary interference.

350. The Court has distinguished between different methods of investigation which result in different levels of intrusion into an individual's private life. According to the Court, the interception of communications represents one of the gravest intrusions, as it is capable of disclosing more information on a person's conduct, opinions or feelings (see *Uzun v. Germany*, no. 35623/05, § 52, ECHR 2010 (extracts))). Consequently, in *Uzun* the Court found that the interception of communications represented a greater intrusion into an individual's private life than the tracking of his vehicle via GPS (see *Uzun*, cited above, § 52). In *Ben Faiza v. France*, no. 31446/12, 8 February 2018, it further distinguished between the tracking of a vehicle, which nevertheless made it possible to geolocate a person in real time, and the lower level of intrusion occasioned by the transmission to

a judicial authority of existing data held by a public or private body (see *Ben Faiza*, cited above, § 74).

351. However, thus far the Court has only declined to apply the minimum requirements test in secret surveillance cases which did not involve the interception of communications, and in which the degree of intrusion was not considered to be comparable to that caused by interception (see for example, *R.E. v. the United Kingdom*, no. 62498/11, 27 October 2015 and *Uzun*, cited above).

352. In any event, it is not necessary for the Court to decide whether the six minimum requirements apply to the interception of communications data since, save for the section 16 safeguards, the section 8(4) regime treats intercepted content and related communications data in the same way. It will therefore focus its attention on whether the justification provided by the Government for exempting related communications data from this safeguard is proportionate to the legitimate aim pursued; that is, ensuring the effectiveness of that safeguard in respect of content.

353. It is not in doubt that communications data is a valuable resource for the intelligence services. It can be analysed quickly to find patterns that reflect particular online behaviours associated with activities such as a terrorist attack and to illuminate the networks and associations of persons involved in such attacks, making it invaluable in fast-moving operations; and, unlike much data relating to content, it is not generally encrypted (see paragraphs 158, 163, 169, 176 and 301 above).

354. Furthermore, the Court accepts that the effectiveness of the section 16(2) safeguard depends on the intelligence services having a means of determining whether a person is in the British Islands, and access to related communications data would provide them with that means.

355. Nevertheless, it is a matter of some concern that the intelligence services can search and examine "related communications data" apparently without restriction. While such data is not to be confused with the much broader category of "communications data", it still represents a significant quantity of data. The Government confirmed at the hearing that "related communications data" obtained under the section 8(4) regime will only ever be traffic data. However, according to paragraphs 2.24-2.27 of the ACD Code (see paragraph 117 above), traffic data includes information identifying the location of equipment when a communication is, has been or may be made or received (such as the location of a mobile phone); information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication; routing information identifying equipment through which a communication is or has been transmitted (for example, dynamic IP address allocation, file transfer logs and e-mail headers (other than the subject line of an e-mail, which is classified as content)); web browsing information to the extent that only a host machine, server, domain name or IP address is disclosed (in

other words, website addresses and Uniform Resource Locators ("URLs") up to the first slash are communications data, but after the first slash content); records of correspondence checks comprising details of traffic data from postal items in transmission to a specific address, and online tracking of communications (including postal items and parcels) (see paragraph 117 above).

356. In addition, the Court is not persuaded that the acquisition of related communications data is necessarily less intrusive than the acquisition of content. For example, the content of an electronic communication might be encrypted and, even if it were decrypted, might not reveal anything of note about the sender or recipient. The related communications data, on the other hand, could reveal the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. In bulk, the degree of intrusion is magnified, since the patterns that will emerge could be capable of painting an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with (see paragraph 301 above).

357. Consequently, while the Court does not doubt that related communications data is an essential tool for the intelligence services in the fight against terrorism and serious crime, it does not consider that the authorities have struck a fair balance between the competing public and private interests by exempting it in its entirety from the safeguards applicable to the searching and examining of content. While the Court does not suggest that related communications data should only be accessible for the purposes of determining whether or not an individual is in the British Islands, since to do so would be to require the application of stricter standards to related communications data than apply to content, there should nevertheless be sufficient safeguards in place to ensure that the exemption of related communications data from the requirements of section 16 of RIPA is limited to the extent necessary to determine whether an individual is, for the time being, in the British Islands.

- *Duration of the secret surveillance measure*

358. Pursuant to section 9 of RIPA (see paragraph 62 above), a section 8(4) warrant ceases to have effect at the end of the "relevant period" unless it is renewed. For warrants issued by the Secretary of State for reasons of national or economic security, the "relevant period" is six months, and for warrants issued by the Secretary of State for the purposes of preventing serious crime, the "relevant period" is three months. These warrants are renewable for periods of six and three months respectively. Warrants may be renewed at any point before their expiry date by application to the Secretary of State. The application must contain the same

information as the original application; it must also contain an assessment of the value of the interception to date and explain why the continuation of interception is necessary, within the meaning of section 5(3), and proportionate (see paragraph 6.22-6.24 of the IC Code at paragraph 90 above). Paragraph 6.7 of the IC Code requires regular surveys of relevant communications links (see paragraph 90 above). Consequently, any application for renewal of a warrant would have to show that interception of those links continued to be of value, and continued to be necessary and proportionate (in the Convention sense).

359. Furthermore, the Secretary of State must cancel a warrant if satisfied that it is no longer necessary on section 5(3) grounds (see section 9 of RIPA at paragraph 62 above).

360. In *Kennedy* (cited above, § 161) the Court considered the same provisions on the duration and renewal of interception warrants (in that case, in the context of the section 8(1) regime) and found that the rules were sufficiently clear as to provide adequate safeguards against abuse. In particular, it noted that the duty on the Secretary of State to cancel warrants which were no longer necessary meant, in practice, that the intelligence services had to keep their warrants under continuous review. In light of the foregoing considerations, the Court sees no grounds upon which to reach a different conclusion in the present case. In particular, it sees no evidence to substantiate the applicants' claim that once issued, section 8(4) warrants could continue indefinitely regardless of whether they continued to be necessary and proportionate.

- Procedure to be followed for storing, accessing, examining and using the intercepted data

361. As already noted, analysts may only examine material which appears on the automatically generated index. Prior to analysts being able to read, look at or listen to material on the index, they must make a record of why access to the material is necessary for one of the statutory purposes set out in section 5(3) of RIPA, and proportionate, having regard to whether the information could reasonably be obtained by less intrusive means (see section 16 of RIPA, at paragraph 79 above, and paragraph 7.15 of the IC Code, at paragraph 90 above). Pursuant to section 16(2), they cannot select material for examination using criteria that refer to the communications of individuals known currently to be in the British Islands (see paragraph 79 above). Paragraph 7.16 of the IC Code also requires the analyst to indicate any circumstances likely to give rise to a degree of collateral infringement of privacy, together with the measures taken to reduce the extent of that intrusion (see paragraph 90 above). Subsequent access by the analyst is limited to a defined period of time; although that period of time may be renewed, the record must be updated giving reasons for renewal (see paragraph 7.17 of the IC Code, at paragraph 90 above).

362. Paragraph 7.15 of the IC Code further requires that analysts examining intercepted material must be specially authorised to do so; must receive regular mandatory training regarding on the provisions of RIPA and specifically the operation of section 16 and the requirements of necessity and proportionality; and must be vetted (see paragraph 90 above). Furthermore, regular audits are carried out which must include checks to ensure that the records requesting access to material have been compiled correctly, and that the material requested falls within the matters certified by the Secretary of State (see paragraph 7.18 of RIPA, at paragraph 90 above).

363. With regard to the storage of intercepted material, paragraph 7.7 of the IC Code requires that prior to its destruction, it must be stored securely and must not be accessible to persons without the required level of security clearance (see paragraph 90 above).

364. In light of the foregoing, and subject to its conclusions at paragraph 347 and 357 above, the Court would accept that the provisions relating to the storing, accessing, examining and using intercepted data are sufficiently clear.

- Procedure to be followed for communicating the intercepted data to other parties

365. While material is being stored, section 15(2) of RIPA and paragraphs 7.2 of the IC Code require that the following are limited to the minimum necessary for the "authorised purposes": the number of persons to whom the material or data is disclosed or made available; the extent to which the material or data is disclosed or made available; the extent to which the material or data is copied; and the number of copies that are made (see paragraphs 72-77 and 90 above). Pursuant to section 15(4) and paragraph 7.2 of the IC Code, something is necessary for the authorised purposes if, and only if, it continues to be, or is likely to become, necessary for the purposes mentioned in section 5(3) of RIPA; for facilitating the carrying out of any of the interception functions of the Secretary of State; for facilitating the carrying out of any functions of the Interception of Communications Commissioner or of the IPT; to ensure 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; or for the performance of any duty imposed on any person under public records legislation (see paragraphs 72-77 and 90 above).

366. Paragraph 7.3 of the IC Code prohibits disclosure to persons who have not been appropriately vetted 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 or she needs to know about the intercepted material to carry out those duties (see paragraph 90 above). In the same way, only so much of the intercepted material may be disclosed as the recipient needs. Paragraph 7.3 applies

equally to disclosure to additional persons within an agency, and to disclosure outside the agency. Pursuant to paragraph 7.4, it also applies not just to the original interceptor, but also to anyone to whom the intercepted material is subsequently disclosed (see paragraph 90 above).

367. According to paragraph 7.5 of the IC Code, where intercepted material is disclosed to the authorities of a country or territory outside the United Kingdom, 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. 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 (see paragraph 90 above).

368. The Court considered very similar provisions in *Kennedy*; although paragraph 7.5 is new, paragraphs 7.3, 7.4 and 7.6 in the 2016 IC Code are identical to paragraphs 6.4, 6.5 and 6.6 of the previous version. It was satisfied that the provisions on processing and communication of intercept material provided adequate safeguards for the protection of data obtained (see *Kennedy*, cited above, § 163). In the present case, however, the applicants have expressed concern about an aspect of the procedure which was not addressed in *Kennedy*; namely, the requirement that disclosure and copying be "limited to the minimum necessary for the 'authorised purposes'", when something might be considered "necessary" for an "authorised purpose" if it was "likely to become necessary". As "likely to become necessary" is not further defined in RIPA or the IC Code, or indeed anywhere else, it could in practice give the authorities a broad power to disclose and copy intercept material. Nevertheless, it is clear that even if disclosure or copying is "likely to become necessary" for an "authorised purpose", the material can still only be disclosed to a person with the appropriate level of security clearance, who has a "need to know". Furthermore, only so much of the intercept material as the individual needs to know is to be disclosed; where a summary of the material would suffice, then only a summary should be disclosed.

369. Therefore, while it would be desirable for the term "likely to become necessary" to be more clearly defined in either RIPA or the IC Code, the Court considers that, taken as a whole, section 15 of RIPA and Chapter 7 of the IC Code provide adequate safeguards for the protection of data obtained.

- The circumstances in which intercept material must be erased or destroyed

370. Section 15(3) of RIPA and paragraph 7.8 of the IC Code require that every copy of intercepted material or data (together with any extracts

and summaries) be destroyed securely as soon as retention is no longer necessary for any of the section 5(3) purposes (see paragraphs 74 and 90 above). In practice, this means that intercepted material which is filtered out in near real-time is destroyed. Similarly, following the application of selectors and search criteria, material which is not added to the analyst's index is also destroyed (see paragraphs 72-77 and 90 above).

371. Paragraph 7.9 provides that where an intelligence service receives unanalysed intercepted material and related communications data from interception under a section 8(4) warrant, it must specify maximum retention periods for different categories of the data which reflect its nature and intrusiveness. These specified periods should normally be no longer than two years, and should be agreed with the Interception of Communications Commissioner. 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 (see paragraphs 72-77 above). Pursuant to paragraph 7.8, if intercepted 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 (see paragraph 90 above).

372. According to the 2016 annual report of the Interception of Communications Commissioner, every interception agency had a different view on what constituted an appropriate retention period for intercepted material and related communications data. The retention periods for content ranged between thirty days and one year and the retention periods for related communications data ranged between six months and one year (see paragraph 186 above). Therefore, while the specific retention periods are not in the public domain, it is clear that they cannot exceed two years and, in practice, they do not exceed one year (with much content and related communications data being retained for significantly shorter periods).

373. Furthermore, where an application is lodged with the IPT, it can examine whether the time-limits for retention have been complied with and, if they have not, it may find that there has been a breach of Article 8 of the Convention and order the destruction of the relevant material. Where the retention has resulted in damage, detriment or prejudice, compensation may also be awarded. In the *Liberty* proceedings, brought by the applicants in the third of the joined cases, the IPT found that there had been a breach of Article 8 of the Convention by virtue of the fact that email communications of Amnesty International, which had been intercepted and accessed "lawfully and proportionately", had nevertheless been retained for longer than was permitted under GCHQ's internal policies. GCHQ was ordered to destroy the communications within seven days, and to provide a closed report within fourteen days confirming their destruction. A hard copy of the communications was to be delivered to the Commissioner (see paragraph 54 above).

374. Therefore, in the Court's view the provisions on the erasure and destruction of intercept material are also sufficiently clear.

- *Supervision, notification and remedies*

375. Supervision of the regime is carried out at a number of levels. First of all, according to the Interception of Communications Commissioner, a "critical quality assurance function [is] initially carried out by the staff and lawyers within the intercepting agency or the warrant-granting department" (see paragraph 180 above). The warrant-granting departments provide independent advice to the Secretary of State and perform important pre-authorisation scrutiny of warrant applications and renewals to ensure that they were (and remained) necessary and proportionate (see paragraph 180 above).

376. Secondly, section 8(4) warrants must be authorised by the Secretary of State. As already noted, while the Court has recognised judicial authorisation to be an "important safeguard against arbitrariness" (see *Roman Zakharov*, cited above, § 249), to date it has not considered it to be a "necessary requirement" (see, for example, *Roman Zakharov*, cited above, § 258; see also *Klass and Others*, cited above, § 51; *Weber and Saravia*, cited above, § 115; *Kennedy*, cited above, § 31; and *Szabó and Vissy*, cited above, § 77*).* Although desirable in principle, by itself it is neither necessary nor sufficient to ensure compliance with Article 8 of the Convention (see paragraphs 318-320 above).

377. It is true that the Court has generally required a non-judicial authority to be sufficiently independent of the executive (see *Roman Zakharov*, cited above, § 258). However, it must principally have regard to the actual operation of a system of interception as a whole, including the checks and balances on the exercise of power, and the existence (or absence) of any evidence of actual abuse (see paragraph 320 above), such as the authorising of secret surveillance measures haphazardly, irregularly or without due and proper consideration (see *Roman Zakharov*, cited above, § 267).

378. In the present case there is no evidence to suggest that the Secretary of State was authorising warrants without due and proper consideration. The authorisation procedure was subject to independent oversight by the Interception of Communications Commissioner (recently replaced by the Investigatory Powers Commissioner following the coming into force of the Investigatory Powers Act 2016 – see paragraph 147 above), who was independent of the executive and the legislature, held or had held high judicial office, and was tasked with overseeing the general functioning of the surveillance regime and the authorisation of interception warrants in specific cases. The Commissioner reported annually to the Prime Minister and his report was a public document (subject to the non-disclosure of confidential annexes) which was laid before Parliament. In undertaking his

review of surveillance practices, he was granted access to all relevant documents, including closed materials, and all those involved in interception activities had a duty to disclose to him any material he required. The obligation on the intelligence services to keep records ensured that he had effective access to details of surveillance activities undertaken (see paragraph 145 above). In 2016, 970 warrants were examined during twenty-two interception inspections, representing 61% of the number of warrants in force at the end of the year and 32% of the total of new warrants issued in 2016 (see paragraph 185 above). As a consequence, in *Kennedy* the Court accepted that despite the fact that the section 8(1) warrant was authorised by the Secretary of State, sufficient independence was provided by the Interception of Communications Commissioner (see *Kennedy*, cited above, § 166).

379. Furthermore, the IPT has extensive jurisdiction to examine any complaint of unlawful interception: unlike in many other countries, its jurisdiction does not depend on notification of the interception to its subject (see paragraph 124 above), which means that any person who believes that he or she has been subject to secret surveillance may make an application to it (see paragraph 318 above). Its members must hold or have held high judicial office or be a qualified lawyer of at least ten years' standing (see paragraph 123 above). Those involved in the authorisation and execution of an intercept warrant are required to disclose to it all the documents it may require, including "below the waterline" documents which could not be made public for reasons of national security (see paragraph 127 above); it has discretion to hold oral hearings, in public, where possible (see paragraphs 131, 138 and 139 above); in closed proceedings it may appoint Counsel to the Tribunal also to make submissions on behalf of claimants who cannot be represented (see paragraph 142 above); and when it determines a complaint it has the power to award compensation and make any other order it sees fit, including quashing or cancelling any warrant and requiring the destruction of any records (see paragraph 128 above). The publication of the IPT's legal rulings further enhances the level of scrutiny afforded to secret surveillance activities in the United Kingdom (see *Kennedy*, cited above, § 167).

380. In any case, the Court notes that under the new Investigatory Powers Act 2016 warrants will have to be approved by judicial commissioners following their authorisation by the Secretary of State. Although this new procedure has not yet been implemented, the Investigatory Powers Commissioner and the deputy Investigatory Powers Commissioner have been appointed (see paragraph 197 above).

381. Therefore, while the Court considers judicial authorisation to be highly desirable and, in its absence, will generally require a non-judicial authority to be independent of the executive, in the present case, in view of the pre-authorisation scrutiny of warrant applications, the extensive post-

authorisation scrutiny provided by the (independent) Commissioner's office and the IPT, and the imminent changes to the impugned regime, it would accept that the authorisation of section 8(4) warrants by the Secretary of State does not, in and of itself, give rise to a breach of Article 8 of the Convention.

382. Finally, the Court recalls that in light of the Edward Snowden revelations, there were three thorough independent reviews of the existing interception regimes, and none of the reviewing bodies found any evidence that deliberate abuse of interception powers was taking place (see paragraphs 148-172 above).

383. In light of the above considerations, the Court is of the opinion that the supervision and oversight of the bulk interceptions capable of providing adequate and effective guarantees against abuse.

- *Proportionality*

384. With regard to the proportionality of the bulk interception regime, the Court notes that the Independent Reviewer of Terrorism Legislation, examined a great deal of closed material and concluded that bulk interception was an essential capability: first, because terrorists, criminals and hostile foreign intelligence services had become increasingly sophisticated at evading detection by traditional means; and secondly, because the nature of the global Internet meant that the route a particular communication would travel had become hugely unpredictable. Although he and his team (including a person with the necessary technical background to understand the systems and techniques used by GCHQ, and the uses to which they could be put, an investigator with experience as a user of secret intelligence, including intelligence generated by GCHQ, and senior independent counsel with the skills and experience to challenge forensically the evidence and the case studies presented by the security and intelligence services) looked at alternatives to bulk interception (including targeted interception, the use of human sources and commercial cyber-defence products), they concluded that no alternative or combination of alternatives would be sufficient to substitute for the bulk interception power (see paragraph 176 above).

385. Similarly, while acknowledging the risks that bulk interception can pose for individual rights, the Venice Commission nevertheless recognised its intrinsic value for security operations, since it enabled the security services to adopt a proactive approach, looking for hitherto unknown dangers rather than investigating known ones (see paragraph 211 above).

386. The Court sees no reason to disagree with the thorough examinations carried out by these bodies and the conclusions subsequently reached. It is clear that bulk interception is a valuable means to achieve the legitimate aims pursued, particularly given the current threat level from both global terrorism and serious crime.

(γ) Conclusions

387. In light of the foregoing considerations, the Court considers that the decision to operate a bulk interception regime was one which fell within the wide margin of appreciation afforded to the Contracting State. Furthermore, in view of the independent oversight provided by the Interception of Communications Commissioner and the IPT, and the extensive independent investigations which followed the Edward Snowden revelations, it is satisfied that the intelligence services of the United Kingdom take their Convention obligations seriously and are not abusing their powers under section 8(4) of RIPA. Nevertheless, an examination of those powers has identified two principal areas of concern; first, the lack of oversight of the entire selection process, including the selection of bearers for interception, the selectors and search criteria for filtering intercepted communications, and the selection of material for examination by an analyst; and secondly, the absence of any real safeguards applicable to the selection of related communications data for examination.

388. In view of these shortcomings and to the extent just outlined, the Court finds that the section 8(4) regime does not meet the "quality of law" requirement and is incapable of keeping the "interference" to what is "necessary in a democratic society". There has accordingly been a violation of Article 8 of the Convention.

B. The intelligence sharing regime

389. The applicants in the third of the joined cases complain that the respondent State's receipt of material intercepted by the NSA under PRISM and Upstream was in breach of their rights under Article 8 of the Convention. The applicants in the first of the joined cases complain more generally about the receipt of information from foreign intelligence services.

1. Admissibility

(a) The parties' submissions

390. The Government argued that the applicants could not claim to be victims of the alleged violation within the meaning of Article 34 of the Convention since they could not possibly have been affected by the intelligence sharing regime. They did not contend, and had put forward no evidential basis for contending, that their communications had in fact been intercepted under PRISM/Upstream and subsequently shared with the United Kingdom intelligence services. Rather, they asserted only that their communications "might have been" subject to foreign interception conveyed to United Kingdom authorities, or that they "believed" that to be the case. As such, their complaint was an abstract one about the regime

itself, and the Court should not entertain an abstract challenge when the applicants had available to them an effective remedy in the form of the IPT.

391. The applicants, on the other hand, submitted that on account of their global public interest activities and the very broad range of persons and organisations with which they were in contact, they were at genuine risk of having their communications obtained by a foreign intelligence service and requested by the United Kingdom authorities. They further submitted that there was no adequate remedy available under domestic law for the alleged breach of their Convention rights.

(b) The Court's assessment

392. The Court has accepted that an applicant could 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 were satisfied: first, the Court would examine whether the applicant could possibly be affected by the legislation permitting secret surveillance measures; and secondly, it would take into account the availability of remedies at the national level and adjust the degree of scrutiny depending on the effectiveness of such remedies. Where the domestic system did not afford an effective remedy, there would be a greater need for scrutiny by the Court and the individual would not need to demonstrate the existence of any risk that secret surveillance measures were applied to him. By contrast, if the national system provides for effective remedies, the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting 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 (*Roman Zakharov*, cited above, § 171).

393. In the present case the Court has accepted that the IPT offers an effective remedy to anyone who wishes to complain about an interference with his or her communications by the United Kingdom authorities (see paragraphs 250-266 above).It has jurisdiction to investigate any complaint that a person's communications have been intercepted and, where interception has occurred, to examine the authority for such interception (see paragraph 124 above). This jurisdiction clearly extends to complaints about the receipt of intelligence from foreign intelligence services. Indeed, in the *Liberty* proceedings the IPT considered the applicants' complaints about both the section 8(4) regime and the intelligence sharing regime with equal diligence (see paragraphs 32-40 above). Consequently, the applicants can only claim to be "victims" on account of the mere existence of the intelligence sharing regime if they are able to show that, due to their personal situation, they were potentially at risk of having their communications obtained by the United Kingdom authorities through a

request to a foreign intelligence service (see *Roman Zakharov*, cited above, § 171).

394. According to Chapter 12 of the IC Code, absent exceptional circumstances intelligence can only be requested from third countries where there is already a section 8(1) or section 8(4) warrant in place. This means that there must either be an Article 8(1) warrant in relation to the subject at issue, or a section 8(4) warrant and accompanying certificate which covers the subject's communications (see paragraph 90 above). However, section 8(4) warrants are relatively broad in scope, and the Court has already considered the general terms in which both warrants and accompanying certificates are drafted (see paragraphs 156 and 341 above). Moreover, it is clear from the *Liberty* proceedings that at least two of the applicants in the third of the joined cases had their communications lawfully intercepted and selected for examination by the United Kingdom intelligence services under the section 8(4) regime (see paragraphs 54 and 55 above). While there is no reason to believe that these applicants were themselves of interest to the intelligence services, their communications could have been obtained lawfully under the section 8(4) regime if, as they claim, they were in contact with persons who were. Similarly, their communications could lawfully be requested from a third country under the intelligence sharing regime if they were in contact with an individual who was the subject of a request.

395. The Court would therefore accept, on the basis of the information submitted to it, that the applicants were potentially at risk of having their communications requested from a foreign intelligence service. In addition, it would accept that they were also potentially at risk of having their communications obtained by a foreign intelligence service. Although the United States of America is not the only country from which the authorities of the respondent State might request intelligence, the submissions before this Court – and before the IPT – focused on the receipt of information from the NSA. While PRISM is a targeted scheme which allows intelligence material to be obtained from Internet Service Providers ("ISPs"), Upstream appears to be a bulk interception scheme similar to the section 8(4) regime. In other words, it permits broad access to global data, in particular that of non-US citizens, which can then be collected, stored and searched using keywords.

396. In light of the foregoing considerations, the Court would accept that the applicants were potentially at risk of having their communications obtained by the intelligence services of the respondent State under the intelligence sharing regime. As such, it finds that they can claim to be victims, within the meaning of Article 34 of the Convention, of the violation alleged to flow from the intelligence sharing regime.

397. The Court notes that this complaint is not manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention. It further notes

that it is not inadmissible on any other grounds. It must therefore be declared admissible.

2. Merits

(a) The parties' submissions

(i) The applicants

398. The applicants submitted that even following the 9 October disclosure, there remained no basis in law for the intelligence sharing carried out by the intelligence services, and there was certainly no regime which satisfied the Court's "quality of law" requirements.

399. With regard to the test to be applied, the applicants contended that an interference with the rights protected by Article 8 of the Convention was no less serious when a third State shared the intelligence with the respondent State than when the respondent State conducted the surveillance itself. In *R.E.* the Court held that in determining whether the six minimum requirements applied the decisive factor would be the level of interference with an individual's right to respect for his or private life, and not the technical definition of that interference (*R.E.*, cited above, § 130). Since the degree of interference caused by the receipt of intelligence from third countries was similar to that caused by direct interception on the part of the respondent State, how that interference was technologically achieved should be irrelevant.

400. In the opinion of the applicants, the publication of the revised IC Code in 2016 was insufficient the remedy the flaws in the regime identified by the IPT as it simply applied the inadequate RIPA regime to the obtaining of data intercepted by a foreign Government.

(ii) The Government

401. The Government submitted that the intelligence sharing regime now had a basis in domestic law (namely, the Security Services Act 1989 ("the SSA") and the Intelligence Services Act 1994 ("the ISA"), as read with the Counter Terrorism Act 2008 ("the CTA"); the Human Rights Act 1998 ("the HRA"); the Data Protection Act 1998 ("the DPA"); the Official Secrets Act 1989 ("the OSA"); and Chapter 12 of the IC Code) and that law was clearly accessible.

402. They further argued that it was foreseeable as the law indicated the scope of any discretion and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference. They did not accept that the six criteria set down in *Weber and Saravia* (see paragraph 307 above) applied to an intelligence sharing regime in the same way as they applied to an interception regime. In this regard, the Court had expressly recognised that the strict standards developed in intercept cases

did not necessarily apply in other surveillance cases (for example, *Uzun*, cited above). While some of the material obtained from foreign governments might be the product of intercept, that would not necessarily be the case and the intelligence services might not even know whether communications provided to them by a foreign Government were the product of intercept.

403. Even if the six minimum requirements did apply, the Government argued that they were satisfied. First, the regime was sufficiently clear as regards the circumstances in which the intelligence services could in principle obtain information from other States; they could only obtain information so far as it was necessary for the proper discharge of their functions, being the interests of national security, the economic well-being of the United Kingdom, and the prevention and detection of serious crime.

404. Moreover, the circumstances in which the intelligence agencies could obtain information under the intelligence sharing regime were defined and circumscribed by the IC Code. In this regard, the effect of Chapter 12 of the Code was to confirm that, other than in exceptional circumstances, the intelligence services could only request "raw intercept" from a foreign government if it concerned targets who were already the subject of an interception warrant under Part I of RIPA, that material could not be obtained by the intelligence services themselves, and it was necessary and proportionate to obtain it. In the absence of a warrant, a request could only be made if it did not amount to a deliberate circumvention, or otherwise frustrate the objectives, of RIPA. Furthermore, any request made in the absence of a warrant would be decided on by the Secretary of State personally, and if the request was for "untargeted" material, communications obtained could not be examined according to any of the factors mentioned in section 16(2) of RIPA.

405. The Government further contended that the intelligence sharing regime was sufficiently clear as regards the subsequent handling, use and possible onward disclosure of material. Not only were the intelligence services bound by the general constraints of proportionality in the HRA and the fifth and seventh data protection principles, but Chapter 12 of the IC Code also provided that intercepted communications data or content received from another State, regardless of whether it was solicited or unsolicited, analysed or unanalysed, was subject to exactly the same rules and safeguards as material obtained directly by the intelligence services by interception under RIPA. In other words, the safeguards set out in section 15 of RIPA also applied to intercept material obtained under the intelligence sharing regime.

406. Finally, the Government pointed out that the intelligence sharing regime was subject to the same oversight mechanisms as the section 8(4) regime, and none of these oversight bodies had revealed any deliberate abuse by the intelligence services of their powers. Furthermore, no evidence

was found to suggest that the intelligence services had – or had attempted – to use the intelligence sharing regime to circumvent RIPA.

(b) The submissions of the third parties

(i) The Electronic Privacy Information Center ("EPIC")

407. EPIC submitted that the evolving technologies of the NSA and other intelligence agencies had created an almost unlimited ability to access, store and use personal information and private communications globally. However, no US law or regulation prohibited the NSA from conducting warrantless surveillance on foreign citizens abroad. Furthermore, in recent years the US had failed to adopt any meaningful reforms which would have provided adequate privacy and data protection safeguards for non-US persons.

(ii) Access Now

408. Access Now contended that while Mutual Legal Assistance Treaties ("MLATs") offered a transparent and formal process for one State party to request intelligence for another, the operation of secret signals intelligence programmes (for example, the Five Eyes intelligence sharing network of which the United Kingdom, the US, Australia, Canada and New Zealand were members) were not transparent and were prohibited by international human rights standards. Such secret programmes were not necessary, since the relevant intelligence could be obtained under MLATs.

(iii) Bureau Brandeis

409. The members of the Bureau Brandeis coalition were plaintiffs in a case against the Netherlands. The Dutch authorities had accepted that data was exchanged with foreign intelligence partners (including the US) and that it could not be excluded that they had received information acquired by foreign services using methods that might infringe human rights. The coalition brought proceedings in which they argued that the NSA's mass data collection programs violated human rights guaranteed by the Convention. However, the Hague District Court said that under Dutch law, Dutch intelligence services were allowed to collaborate with the NSA, and the NSA was in turn bound by US law which, in general, did not conflict with the Convention's privacy requirements. The court further held that because the raw data was shared in bulk, less stringent safeguards were necessary than would apply when the data was examined and used, as there was a difference between receiving data and using it for individual cases. An appeal against this decision was dismissed in March 2017.

410. In their third party intervention before this Court, the coalition argued that the sharing of intelligence should only be permitted if it was accompanied by sufficient safeguards and the foreign authority had a sound

legal basis for capturing the material. Otherwise, there could be a circumvention of the protection provided by Article 8 of the Convention. In other words, States should not be allowed to obtain material from foreign authorities that they could not lawfully capture themselves.

(iv) Center for Democracy and Technology ("CDT") and Pen American Center ("PEN America")

411. CDT and PEN America submitted that the interception regimes operated by the NSA would satisfy neither the "in accordance with the law" nor the "proportionality" requirements of Article 8 of the Convention, and these deficiencies tainted the lawfulness of the United Kingdom's intelligence sharing regime.

(v) The International Commission of Jurists ("ICJ")

412. The ICJ referred the Court to Articles 15 and 16 of the Articles of State Responsibility of the International Law Commission ("the ILC Articles"). They contended that, pursuant to Article 15, a Contracting State could be responsible for mass surveillance conducted by a non-Contracting State if they were acting in organised and structured forms of co-operation; and that, pursuant to Article 16, a Contracting State could be responsible for mass surveillance conducted by a non-Contracting State if it contributed to the surveillance programme and had actual or constructive knowledge of the breaches of international human rights obligations inherent in the system. The ICJ further submitted that Contracting States participating in or contributing to a mass surveillance programme were obliged to establish a system of safeguards for the protection of Article 8 rights, and were also under a duty to protect persons within their jurisdiction from violations of Article 8 rights caused by mass surveillance programmes.

(vi) Open Society Justice Initiative ("OSJI")

413. OSJI argued that States should not receive or request data from a third party in a manner that circumvents individuals' Article 8 rights. To ensure that this does not happen, they must put in place safeguards at the point when the material is first gathered, including prior scrutiny of the human rights record and interception laws and practices in the foreign State, and independent, preferably judicial, *a posteriori* oversight of any sharing arrangements to ensure that the safeguards are in place and enforced.

(vii) The Law Society of England and Wales

414. The Law Society previously submitted that the RIPA regime and associated Codes provided no robust or transparent safeguards for legally privileged material. Since the same safeguards applied to privileged material obtained by foreign States and disclosed to the intelligence services of the United Kingdom, the same deficiencies also tainted that regime.

(viii) Human Rights Watch ("HRW")

415. Although the present applications focused on the receipt of foreign intelligence from the United States, HRW believed that the network of States with which communications intelligence was shared was vastly larger. For example the "Five Eyes Alliance" comprised the United Kingdom, the United States, Australia, Canada and New Zealand, and there were also thought to be other, more restricted intelligence sharing coalitions (for example, the "Nine Eyes", adding Denmark, France, the Netherlands and Norway; the "Fourteen Eyes", adding Germany, Belgium, Italy, Spain and Sweden; and the "Forty-One Eyes", adding in others in the allied coalition in Afghanistan).

(c) The Court's assessment

(i) The scope of the applicants' complaints

416. This is the first time that the Court has been asked to consider the Convention compliance of an intelligence sharing regime. While the operation of such a scheme might raise a number of different issues under the Convention, in the present case the applicants' complaints focus on the Article 8 compliance of the regime by which the United Kingdom authorities request and receive intelligence from foreign Governments. The applicants do not complain about the transfer of intelligence from the United Kingdom intelligence services to foreign counterparts; nor do they invoke any other Convention Articles.

417. In the *Liberty* proceedings (in which the IPT was only concerned with the receipt of information from the United States) the applicants submitted that information acquired from the NSA fell into three categories: material which the NSA had provided to the United Kingdom intelligence services unsolicited, and which on its face derived from intercept; communications which the United Kingdom intelligence services had either asked the NSA to intercept, or to make available to them as intercept; and material obtained by the NSA other than by the interception of communications. Although the complaint before the Court is somewhat wider than the one which was before the IPT, the applicants in the first of the joined cases having complained about the receipt of information from any foreign Government, the categories identified by the IPT are nevertheless apposite. As the Government, at the hearing, informed the Court that it was "implausible and rare" for intercept material to be obtained "unsolicited", the Court will restrict its examination to material falling into the second and third categories.

418. Material falling within the second category can be divided into two sub-categories: communications which the respondent State has asked a foreign intelligence service to intercept; and communications already intercepted by a foreign intelligence service, which are conveyed to the

authorities of the respondent State upon their request. The Court will first deal with these two sub-categories together, before proceeding to consider the third category separately.

(ii) The nature of the interference

419. The Court has already found that the applicants can claim to be victims of the alleged violation of Article 8 of the Convention occasioned by the existence of an intelligence sharing regime. However, it is important to clarify at the outset the nature of the interference under consideration.

420. Although the impugned regime concerns intercepted communications, the interference under consideration in this case does not lie in the interception itself, which did not, in any event, occur within the United Kingdom's jurisdiction, and was not attributable to that State under international law. As the communications are being intercepted by foreign intelligence agencies, their interception could only engage the responsibility of the respondent State if it was exercising authority or control over those agencies (see, for example, *Jaloud v. the Netherlands* [GC], no. 47708/08, §§ 139 and 151 ECHR 2014 and *Al-Skeini and Others v. the United Kingdom* [GC], no. 55721/07, §§ 130-139, ECHR 2011). Even when the United Kingdom authorities request the interception of communications (rather than simply the conveyance of the product of intercept), the interception would appear to take place under the full control of the foreign intelligence agencies. Some of the third parties have invoked the ILC Articles, but these would only be relevant if the foreign intelligence agencies were placed at the disposal of the respondent State and were acting in exercise of elements of the governmental authority of the respondent State (Article 6); if the respondent State aided or assisted the foreign intelligence agencies in intercepting the communications where that amounted to an internationally wrongful act for the State responsible for the agencies, the United Kingdom was aware of the circumstances of the internationally wrongful act, and the act would have been internationally wrongful if committed by the United Kingdom (Article 16); or if the respondent State exercised direction or control over the foreign Government (Article 17). There is no suggestion that this is the case.

421. Consequently, the interference lies in the receipt of the intercepted material and its subsequent storage, examination and use by the intelligence services of the respondent State.

(iii) The applicable test

422. As with any regime which provides for the acquisition of surveillance material, the regime for the obtaining of such material from foreign Governments must be "in accordance with the law"; in other words, it must have some basis in domestic law, it must be accessible to the person concerned and it must be foreseeable as to its effects (see *Roman Zakharov*,

cited above, § 228). Furthermore, it must be proportionate to the legitimate aim pursued, and there must exist adequate and effective safeguards against abuse. In particular, the procedures for supervising the ordering and implementation of the measures in question must be such as to keep the "interference" to what is "necessary in a democratic society" (see *Roman Zakharov*, cited above, § 232).

423. The parties dispute whether the six minimum requirements commonly applied in cases concerning the interception of communications (namely, the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their communications intercepted; a limit on the duration of interception; 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 intercepted data may or must be erased or destroyed – see paragraph 307 above) should apply in the present case. It is true that the interference in this case is not occasioned by the interception of communications by the respondent State. However, as the material obtained is nevertheless the product of intercept, those requirements which relate to its storage, examination, use, onward dissemination, erasure and destruction must be present. Indeed, as the Venice Commission noted, as States could use intelligence sharing to circumvent stronger domestic surveillance procedures and/or any legal limits which their agencies might be subject to as regards domestic intelligence operations, a suitable safeguard would be to provide that the bulk material transferred could only be searched if all the material requirements of a national search were fulfilled and this was duly authorised in the same way as a search of bulk material obtained by the signals intelligence agency using its own techniques (see paragraph 216 above).

424. Furthermore, while the first and second of the six requirements may not be of direct relevance where the respondent State is not carrying out the interception itself, the Court is nevertheless mindful of the fact that if Contracting States were to enjoy an unfettered discretion to request either the interception of communications or the conveyance of intercepted communications from non-Contracting States, they could easily circumvent their obligations under the Convention. Consequently, the circumstances in which intercept material can be requested from foreign intelligence services must also be set out in domestic law in order to avoid abuses of power. While the circumstances in which such a request can be made may not be identical to the circumstances in which the State may carry out interception itself (since, if a State's own intelligence services could lawfully intercept communications themselves, they would only request this material from foreign intelligence services if it is not technically feasible for them to do so), they must nevertheless be circumscribed sufficiently to prevent –

insofar as possible – States from using this power to circumvent either domestic law or their Convention obligations.

(iv) Application of the test to material falling into the second category

(α) Accessibility

425. The statutory framework which permits the United Kingdom intelligence services to request intercepted material from foreign intelligence agencies is not contained in RIPA. The British-US Communication Intelligence Agreement of 5 March 1946 specifically permits the exchange of material between the United States and the United Kingdom. More generally, the SSA (see paragraphs 98-99 above) and the ISA (see paragraphs 100-103 above) set out the function of the intelligence services and require that there be arrangements for ensuring that no information is obtained by them except so far as necessary for the proper discharge of their functions; and that no information is disclosed by them except so far as necessary for that purpose or for the purpose of any criminal proceedings.

426. Details of the internal arrangements referred to in the SSA and ISA were disclosed during the *Liberty* proceedings (the 9 October disclosure – see paragraphs 26-30 above) and those details have now been incorporated into the most recent IC Code (see paragraph 109 above).

427. Consequently, the Court considers that there is now a basis in law for the requesting of intelligence from foreign intelligence agencies, and that that law is sufficiently accessible. Furthermore, the regime clearly pursues several legitimate aims, including the interests of national security, public safety and the economic well-being of the country, the prevention of disorder or crime, and the protection of the rights and freedoms of others. It therefore falls to the Court to assess the foreseeability and necessity of the regime. As already indicated, it will do so by examining whether the law meets the following requirements by indicating: the circumstances in which intercept material can be requested; the procedure to be followed for examining, using and storing the material obtained; the precautions to be taken when communicating the material obtained to other parties; and the circumstances in which the material obtained must be erased or destroyed (see the third to sixth safeguards referred to in paragraph 307 above).

(β) The circumstances in which intercept material can be requested

428. Chapter 12 of the IC Code (see paragraph 109 above) states that, save in exceptional circumstances, the intelligence services may only make a request to a foreign government for unanalysed intercepted communications and/or associated communications data if an interception warrant under RIPA has already been issued by the Secretary of State, the assistance of the foreign government is necessary to obtain the particular

communications because they cannot be obtained under the existing warrant, and it is necessary and proportionate for the intercepting agency to obtain those communications. A RIPA interception warrant means either a section 8(1) warrant in relation to the subject at issue; a section 8(4) warrant and an accompanying certificate which includes one or more "descriptions of intercepted material" covering the subject's communications; or, where the subject is known to be within the British Islands, a section 8(4) warrant and an accompanying certificate which includes one or more "descriptions of intercepted material" covering his or her communications, together with an appropriate section 16(3) modification.

429. Where exceptional circumstances exist, a request for communications may be made in the absence of a relevant RIPA interception warrant only if it does not amount to a deliberate circumvention of RIPA or otherwise frustrate its objectives (for example, because it is not technically feasible to obtain the communications via RIPA interception), and it is necessary and proportionate for the intercepting agency to obtain those communications. In such a case the request must be considered and decided on by the Secretary of State personally, and, pursuant to the revised IC Code, notified to the Interception of Communications Commissioner (see paragraph 109 above). According to information disclosed during the *Liberty* proceedings, and confirmed in the Government's submissions in the present case, no request for intercept material has ever been made in the absence of an existing RIPA warrant.

430. In light of the above considerations, the Court considers that the circumstances in which the respondent State may request interception or the conveyance of intercepted material are sufficiently circumscribed in domestic law to prevent the State from using this power to circumvent either domestic law or its Convention obligations.

(γ) Procedure to be followed for storing, accessing, examining and using the material obtained

431. By virtue of section 19(2) of the Counter-Terrorism Act 2008 ("CTA" – see paragraph 103), information obtained by any of the intelligence services in connection with the exercise of any of their functions may be used in connection with the exercise of any of their other functions. However, the intelligence services are data controllers for the purposes of the Data Protection Act 1998 and are required to comply with the data protection principles in Part 1 of Schedule 1 to the DPA. While compliance with these principles is subject to exemption by ministerial certificate, they cannot be exempted from the obligation to comply with the fifth and seventh data protection principles, which provide that personal data processed for any purpose shall not be kept for longer than is necessary for that purpose; and 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. A member of the intelligence services commits an offence under section 1(1) of the OSA (see paragraph 107 above) if he discloses, without lawful authority, any information relating to security or intelligence which is, or has been, in his possession by virtue of his position.

432. More specifically, Chapter 12 of the IC Code makes it clear that where intercepted communications content or communications data are obtained by the intelligence services from a foreign government in circumstances where the material identifies itself as the product of an interception, 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 intelligence services as a result of interception under RIPA (see paragraph 109 above). This means that the safeguards in section 15 and 16 of RIPA, as supplemented by Chapter 7 of the IC Code, apply equally to intercepted communications and communications data obtained from foreign governments.

433. The Court has already given careful consideration to the safeguards in section 15 and 16 of RIPA, as supplemented by Chapter 7 of the IC Code, in its assessment of the section 8(4) regime (see paragraphs 361-363 above). In brief, material obtained from foreign intelligence agencies must be stored securely and must not be accessible to persons without the required level of security clearance. Access by the analyst is limited to a defined period of time, and if renewed, the record must be updated giving reasons for renewal. Before being able to examine material obtained from foreign intelligence agencies, specially authorised and vetted analysts must make a record of why access to the material is necessary for one of the statutory purposes set out in section 5(3) of RIPA, and proportionate. They cannot select material for examination using criteria that refer to the communications of individuals known currently to be in the British Islands (unless there is a warrant with a section 16(3) modification, or if, in the absence of a warrant, the Secretary of State has personally considered and approved the examination of those communications by reference to such factors).

434. Although the IPT had, in the *Liberty* proceedings, expressed concern that the section 16(2)(a) and (b) safeguards (which prevent intercepted material being selected for examination by reference to an individual known to be in the British Islands) did not appear to apply to material obtained from foreign governments in the absence of a warrant, the IC Code has since been amended to address this concern. Paragraph 12.5 now expressly provides that if a request made in the absence of a warrant is approved by the Secretary of State other than in relation to specific selectors, any communications obtained must not be examined by the intelligence services 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 (see paragraph 110 above).

435. In light of the foregoing, the Court would accept that the provisions relating to the storing, accessing, examining and using such material are sufficiently clear.

(δ) Procedure to be followed for communicating the material obtained to other parties

436. As with material intercepted directly pursuant to a RIPA warrant (see paragraphs 365-367 above), disclosure of material obtained from foreign intelligence agencies must be limited to the minimum necessary for the "authorised purposes" mentioned in section 5(3) of RIPA. In addition, disclosure to persons who have not been appropriately vetted is prohibited and material may only be disclosed to a person whose duties, which must relate to one of the authorised purposes, are such that he or she needs to know about the material to carry out those duties. In the same way, only so much of the intercepted material may be disclosed as the recipient needs.

437. Section 19(3), (4) and (5) of the CTA further provide that information obtained by MI5 and MI6 for the purposes of any of their functions may be disclosed by them for the purpose of the proper discharge of their functions; in the interests of national security; for the purpose of the prevention or detection of serious crime; or for the purpose of any criminal proceedings. Information obtained by GCHQ may be disclosed by it for the purpose of the proper discharge of its functions or for the purpose of any criminal proceedings (see paragraphs 104-105 above).

438. Moreover, a member of the intelligence services commits an offence under section 1(1) of the OSA 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 (see paragraph 107 above).

439. In light of the foregoing, the Court would also accept that the provisions relating to the procedure to be followed for communicating the material obtained to other parties are sufficiently clear.

(ε) The circumstances in which the material obtained must be erased or destroyed

440. Section 15(3) of RIPA and paragraph 7.8 of the IC Code require that every copy (together with any extracts and summaries) be destroyed securely as soon as retention is no longer necessary for any of the section 5(3) purposes (see paragraphs 74 and 90 above).

(ζ) Supervision and remedies

441. In nearly every case either a section 8(1) or 8(4) warrant will be in place, meaning that the Secretary of State (and, following the coming into force of IPA 2016, a judicial commissioner) will have authorised the interception. In exceptional circumstances, when a warrant is not in place, the Secretary of State must personally consider and decide upon the request, and the Interception of Communications Commissioner (now the Investigatory Powers Commissioner) must be notified. Therefore, in every case where a request has been made the Secretary of State will have deemed the interception to be necessary and proportionate (in the Convention sense).

442. Further oversight of the intelligence sharing regime is provided by the ISC, a cross-party Committee of Members of Parliament which exercises wide powers. Following an extensive review, on 13 July 2013 the ISC published a report in which it concluded that allegations "that GCHQ circumvented UK law by using the NSA's PRISM programme to access the content of private communications" were unfounded as GCHQ had complied with its statutory duties contained in the ISA (see paragraphs 148-150 above).

443. Additional oversight was afforded by the Interception of Communications Commissioner, who was independent from both Government and the intelligence services. He was under a duty by section 58(4) of RIPA to make an annual report to the Prime Minister regarding the carrying out of his functions, which had to be laid before Parliament. As already noted, the Interception of Communications Commissioner has now been replaced by the Investigatory Powers Commissioner. On 17 October 2017, in a reply to a question posed by, *inter alia*, Privacy International, the new Commissioner confirmed that, like his predecessor, he had the power to oversee the Government's intelligence sharing agreements, and that he intended to use those powers actively to ensure effective oversight.

444. A final level of oversight is provided by the IPT, and its effectiveness was demonstrated in the *Liberty* proceedings by the fact that it was able to ensure disclosure of certain arrangements which have now been incorporated into the IC Code (see paragraph 109 above).

(η) Proportionality

445. The Court has always been acutely conscious of the difficulties faced by States in protecting their populations from terrorist violence, which constitutes, in itself, a grave threat to human rights (see, for example, *Lawless v. Ireland (no. 3)*, 1 July 1961, §§ 28–30, Series A no. 3; *Ireland v. the United Kingdom*, 18 January 1978, Series A no. 25; and *Öcalan v. Turkey* [GC], no. 46221/99, § 179, ECHR 2005-IV) and in recent years it has expressly acknowledged – in response to complaints invoking a wide

range of Convention Articles – the very real threat that Contracting States currently face on account of international terrorism (see, for example, *Chahal v. the United Kingdom*, 15 November 1996, § 79, *Reports of Judgments and Decisions* 1996-V; *A. and Others v. the United Kingdom* [GC], no. 3455/05, § 181, ECHR 2009; *A. v. the Netherlands*, no. 4900/06, § 143, 20 July 2010; *Trabelsi v. Belgium*, no. 140/10, § 117, ECHR 2014 (extracts); and *Othman (Abu Qatada) v. United Kingdom*, no. 8139/09, § 183, ECHR 2012).

446. Faced with such a threat, the Court has considered it legitimate for Contracting States to take a firm stand against those who contribute to terrorist acts (see *Othman*, cited above, § 183). Due to the nature of global terrorism, and in particular the complexity of global terror networks, the Court accepts that taking such a stand – and thus preventing the perpetration of violent acts endangering the lives of innocent people – requires a flow of information between the security services of many countries in all parts of the world. As, in the present case, this "information flow" was embedded into a legislative context providing considerable safeguards against abuse, the Court would accept that the resulting interference was kept to that which was "necessary in a democratic society".

(θ) Conclusions

447. In light of the foregoing considerations, the Court considers that the domestic law, together with the clarifications brought by the amendment of the IC Code, indicate with sufficient clarity the procedure for requesting either interception or the conveyance of intercept material from foreign intelligence agencies. In this regard, it observes that the high threshold recommended by the Venice Commission – namely, that the material transferred should only be able to be searched if all the material requirements of a national search were fulfilled and this was duly authorised in the same way as a search of bulk material obtained by the signals intelligence agency using its own techniques – is met by the respondent State's regime. The Court further observes that there is no evidence of any significant shortcomings in the application and operation of the regime. On the contrary, following an investigation the ISC found no evidence whatsoever of abuse.

448. There has accordingly been no violation of Article 8 of the Convention.

(v) Application of the test to material falling into the third category

449. The third category of material identified at paragraph 417 above is material obtained by foreign intelligence agencies other than by the interception of communications. However, as the applicants have not specified the kind of material foreign intelligence agencies might obtain by methods other than interception they have not demonstrated that its

acquisition would interfere with their Article 8 rights. As such, the Court considers that there is no basis upon which it could find a violation of Article 8 of the Convention.

C. The Chapter II regime

450. The applicants in the second of the joined cases complained that the regime for the acquisition of communications data under Chapter II of RIPA was incompatible with their rights under Article 8 of the Convention.

1. Admissibility

451. In both their application to the Court and their initial observations, the applicants in the second of the joined cases incorrectly referred to the Chapter II regime as a regime for the interception of communications data. The Court observes, however, that it is not an interception regime, but rather permits certain public authorities to acquire communications data from Communications Service Providers ("CSPs"). In view of the "fundamental legal misunderstanding" upon which the complaint was originally founded, the Government submitted that the applicants have put forward no factual basis whatsoever for concluding that their communications were acquired in this way, and that they did not contend that they had been affected, either directly or indirectly, by the regime. The Government further argued that neither of the two conditions identified by the Court in *Roman Zakharov* (cited above, § 171) were satisfied in respect of the Chapter II regime: the applicants did not belong to a group "targeted" by the contested legislation, and they had available to them an effective domestic remedy. Consequently, they could not claim to be victims of the alleged violation within the meaning of Article 34 of the Convention.

452. The applicants, on the other hand, submitted that they were entitled to bring the present complaint since they could possibly have been affected by the impugned legislation and no effective remedy was available at the domestic level.

453. In assessing victim status the Court is predominantly concerned with whether an effective remedy existed which permitted a person who suspected that he or she was subject to secret surveillance to challenge that surveillance (see *Roman Zakharov*, cited above, § 171). In the present case, although the Court accepted that there existed special circumstances absolving the applicants from the requirement that they first bring their complaints to the IPT (see paragraph 268 above), it nevertheless found that the IPT was an effective remedy, available in theory and practice, which was capable of offering redress to applicants complaining of both specific incidences of surveillance and the general Convention compliance of surveillance regimes (see paragraphs 250-266 above). Consequently, the applicants can only claim to be "victims" on account of the mere existence

of the Chapter II regime if they are able to show that, due to their personal situation, they were potentially at risk of having their communications data obtained by the United Kingdom authorities through a request to a CSP (see *Roman Zakharov*, cited above, § 171).

454. In this regard, the Court notes that the Chapter II regime is not a regime for the bulk acquisition of communications data; rather, as stated previously, it permits public authorities to request specific communications data. Nevertheless, a large number of public authorities are entitled to make such requests, and the grounds on which a request might be made are relatively wide. Given that the applicants in the second of the joined cases are investigative journalists who have reported on issues such as CIA torture, counterterrorism, drone warfare, and the Iraq war logs, the Court would accept that they were potentially at risk of having their communications obtained by the United Kingdom authorities either directly, through a request to a CSP for their communications data, or indirectly, through a request to a CSP for the communications data of a person or organisation they had been in contact with.

455. The Court would therefore accept that they were "victims" within the meaning of Article 34 of the Convention. As this complaint is not inadmissible on any other grounds, it must be declared admissible.

2. Merits

(a) The parties' submissions

(i) The applicants

456. The applicants submitted that Chapter II of RIPA permitted the obtaining of communications data in a wide range of ill-defined circumstances, without proper safeguards. In particular, they submitted that the legal framework and attendant safeguards were informed by a fundamental but erroneous premise; namely, that the obtaining of communications data was necessarily less intrusive than the interception of content. In particular, the applicants complained that in most cases authorisation for the acquisition of communications data was provided by a designated person, who was not sufficiently independent of the executive or even of the agency requesting the disclosure.

457. Furthermore, they complained that Chapter II provided few limitations as to the basis on which communications data could be acquired, since section 22 of RIPA allowed a designated person to authorise the acquisition of communications data on a broad range of grounds, provided that he or she believed it "necessary". Finally, they argued that there were very few safeguards in respect of the handling and exploitation of communications data.

(ii) The Government

458. The Government pointed out that as the Chapter II regime was a targeted regime, there was nothing "unintentional" about its operation. On the contrary, the acquisition of communications data under it would always be intentional. It was therefore to be distinguished from regimes for the bulk interception or bulk acquisition of data.

459. The Government further argued that the amended Acquisition and Disclosure of Communications Data Code of Practice ("the ACD Code") provided adequate safeguards in respect of the retention of communications data acquired under the Chapter II regime, and that the Interception of Communications Commissioner provided an important degree of oversight of the operation of the regime.

(b) The Court's assessment

(i) Existing case-law on the acquisition of communications data

460. To date, the Court has only twice been called on to consider the Convention compliance of a regime for the acquisition by a public authority of communications data from a CSP: in *Malone* and, more recently, in *Ben Faiza* (both cited above). In *Malone*, the authorities had obtained the numbers dialled on a particular telephone and the time and duration of the calls from the Post Office, which, as the supplier of the telephone service, had acquired this data legitimately by a process known as "metering". While the Court accepted that the use of the data could give rise to an issue under Article 8 of the Convention, it considered that "by its nature" it had to be distinguished from the interception of communications, which was "undesirable and illegitimate in a democratic society unless justified" (see *Malone*, cited above, § 84). However, it was not necessary for the Court to consider this issue in any further detail, since, in the absence of any legal framework governing the acquisition of records from the Post Office, the Court found that the interference had no basis in domestic law (see *Malone*, cited above, § 87).

461. While *Malone* is now thirty-four years old, the *Ben Faiza* judgment was delivered in February 2018. In that case the Court was considering an order issued to a mobile telephone operator to provide lists of incoming and outgoing calls on four mobile telephones, together with the list of cell towers "pinged" by those telephones. Pursuant to the domestic law in question (Article 77-1-1 of the Criminal Procedure Code), prosecutors or investigators could, on the authorisation of the former, require establishments, organisations, persons, institutions and administrations to provide them with documents in their possession which were required for the purposes of the investigation. The Court accepted that the measure was "in accordance with the law", and that the law provided adequate safeguards against arbitrariness. In respect of those safeguards, the Court observed that

a request under Article 77-1-1 was subject to the prior authorisation of the public prosecutor's office; this obligation could not be derogated from under penalty of nullity of the act; and the legality of such a measure could be reviewed in subsequent criminal proceedings against the person concerned and, if found to be unlawful, the criminal courts could exclude the evidence so obtained (*Ben Faiza*, cited above, §§ 72-73).

462. In adopting this approach, the Court distinguished between methods of investigation which made it possible to identify the past geographical position of a person and those which made it possible to geolocate him or her in real time, indicating that the latter was more likely to violate the right to respect for private life. Consequently, in the view of the Court, the transmission to a judicial authority of existing data held by a public or private body was to be distinguished from the establishment of a surveillance system, such as the ongoing monitoring of a telephone line or the placing of a tracking device on a vehicle (*Ben Faiza*, cited above, § 74; see also paragraph 350 above).

463. The Court of Justice of the European Union has also addressed this issue. In *Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources and Others and Settinger and Others* (Cases C-293/12 and C-594/12), the CJEU considered the validity of the Data Retention Directive, and in *Secretary of State for the Home Department v. Watson and Others* (C-698/15), the validity of domestic legislation containing the same provisions as that directive (see paragraphs 224-234 above). While its focus was on the retention of data by CSPs, it also considered the question of access to retained data by the national authorities. In doing so, it indicated that access should be limited to what was strictly necessary for the objective pursued and, where that objective was fighting crime, it should be restricted to fighting serious crime. It further suggested that access should be subject to prior review by a court or independent administrative authority, and that there should be a requirement that the data concerned be retained within the European Union. In light of the CJEU's findings, Liberty sought to challenge Part 4 of the IPA, which included a power to issue "retention notices" to telecommunications operators requiring the retention of data. In response, the Government conceded that Part 4 was incompatible with fundamental rights in EU law since access to retained data was not limited to the purpose of combating "serious crime"; and access to retained data was not subject to prior review by a court or an independent administrative body. The High Court held that the legislation had to be amended by 1 November 2018 (see paragraph 196 above).

(ii) The approach to be taken in the present case

464. The appropriate test in the present case will therefore be whether the Chapter II regime was in accordance with the law; whether it pursued a legitimate aim; and whether it was necessary in a democratic society, having

particular regard to the question of whether it provided adequate safeguards against arbitrariness.

(iii) Examination of the Chapter II regime

465. No interference can be considered to be "in accordance with law" unless the decision occasioning it complies with the relevant domestic law. It is in the first place for the national authorities, notably the courts, to interpret and apply the domestic law: the national authorities are, in the nature of things, particularly qualified to settle issues arising in this connection. The Court cannot question the national courts' interpretation, except in the event of flagrant non-observance or arbitrariness in the application of the domestic legislation in question (see *Mustafa Sezgin Tanrıkulu*, cited above, § 53; see also, *mutatis mutandis*, *Weber and Saravia*, cited above, § 90).

466. The Court observes that the Chapter II regime has a clear basis in both section 22 of RIPA and the ACD Code. However, as a Member State of the European Union, the Community legal order is integrated into that of the United Kingdom and, where there is a conflict between domestic and law and EU law, the latter has primacy. Consequently, the Government have conceded that Part 4 of the IPA is incompatible with EU law because access to retained data was not limited to the purpose of combating "serious crime"; and access to retained data was not subject to prior review by a court or an independent administrative body. Following this concession, the High Court ordered that the relevant provisions of the IPA should be amended by 1 November 2018 (see paragraph 196 above).

467. It is therefore clear that domestic law, as interpreted by the domestic authorities in light of the recent judgments of the CJEU, requires that any regime permitting the authorities to access data retained by CSPs limits access to the purpose of combating "serious crime", and that access be subject to prior review by a court or independent administrative body. As the Chapter II regime permits access to retained data for the purpose of combating crime (rather than "serious crime") and, save for where access is sought for the purpose of determining a journalist's source, it is not subject to prior review by a court or independent administrative body, it cannot be in accordance with the law within the meaning of Article 8 of the Convention.

468. Accordingly, the Court finds that there has been a violation of Article 8 of the Convention.

III. ALLEGED VIOLATION OF ARTICLE 10 OF THE CONVENTION

469. The applicants in the third of the joined cases complained under Article 10 of the Convention about the section 8(4) regime and the intelligence sharing regime, arguing, in particular, that the protection

afforded by Article 10 was of critical importance to them as NGOs involved in matters of public interest, who were exercising a role of public watchdog of similar importance to that of the press; and the applicants in the second of the joined cases, being a journalist and newsgathering organisation, complained under Article 10 of the Convention about both the section 8(4) regime and the Chapter II regime.

470. Article 10 of the Convention provides as follows:

> "1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
>
> 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

A. Admissibility

1. The applicants in the third of the joined cases

471. The Court has already found that as a general rule the IPT has shown itself to be a remedy, available in theory and practice, which is capable of offering redress to applicants complaining about both specific incidences of surveillance and the general Convention compliance of a surveillance regime (see paragraphs 250-266 above). The Court has, however, accepted that there existed special circumstances absolving the applicants in the first and second of the joined cases from the requirement that they exhaust this remedy (see paragraph 268 above), but as the applicants in the third of the joined cases challenged the Convention compliance of both the section 8(4) regime and the intelligence sharing regime before the IPT, they cannot benefit from the "absolution" afforded to the other applicants. Therefore, as they did not complain before the IPT that the intelligence sharing regime was incompatible with Article 10 of the Convention, this complaint must be declared inadmissible for failure to domestic remedies within the meaning of Article 35 § 1 of the Convention.

472. Furthermore, although these applicants did complain before the IPT that the section 8(4) regime was not compatible with Article 10, in doing so they primarily relied on the same arguments invoked in respect of their Article 8 complaint. Insofar as they sought to argue that Article 10 could apply to their investigatory activities as NGOs, this argument was only raised on 17 November 2014 (the first and second open hearings having taken place in July and October 2014). As the IPT considered that this

argument could have been raised at any time, in its judgment it had been raised far too late to be incorporated into the ambit of the *Liberty* proceedings (see paragraph 47 above).

473. Therefore, with regard to the Article 8(4) complaint, the Court finds that insofar as the applicants in the third of the joined cases seek to rely on the special protection afforded by Article 10 of the Convention to journalists, they have not exhausted domestic remedies within the meaning of Article 35 § 1 of the Convention. Their complaints under this head must also be declared inadmissible.

474. Finally, the Court considers that the more general Article 10 complaint – which the applicants raised before the IPT in good time – gives rise to no separate argument over and above that arising out of Article 8 of the Convention. It is not, therefore, necessary to examine this complaint.

2. The applicants in the second of the joined cases

475. As the Court has acknowledged that the applicants in the second of the joined cases were, exceptionally, absolved from the requirement that they first bring their complaints to the IPT, they cannot be said to have failed to exhaust domestic remedies within the meaning of Article 35 § 1 of the Convention. As their complaints are not inadmissible on any other ground, they must, therefore, be declared admissible.

476. Moreover, the applicants in the second of the joined cases are a journalist and a newsgathering organisation, who complain about the interference with confidential journalistic material occasioned by the operation of both the section 8(4) regime and the Chapter II regime. As such, their complaints raise separate issues to those raised under Article 8 of the Convention, which will be examined below.

B. Merits

1. The parties' submissions

(a) The applicants

477. The applicants argued that as freedom of the press constituted one of the essential foundations of a democratic society, and the protection of journalistic sources was one of the cornerstones of freedom of the press, Article 10 of the Convention imposed additional and more exacting requirements where an interference gave rise to a significant risk of revealing journalistic sources or confidential journalistic material. In this regard, they submitted that surveillance measures which ran a significant risk of identifying journalistic source material had to be justified by an "overriding public interest" (*Sanoma Uitgevers B.V.*, cited above, §§ 51 and 90, 14 September 2010 and *Goodwin v. the United Kingdom*, 27 March

1996, § 39 *Reports of Judgments and Decisions* 1996-II); and authorisation could only be granted by a judge or other independent adjudicative body.

478. The applicants submitted that as journalists involved in matters of public interest, who were exercising a role of public watchdog, the protection afforded by Article 10 was of critical importance to them.

479. In respect of the section 8(4) regime, the applicants argued that the interception of material gathered through bulk surveillance was not attended by adequate safeguards. First of all, the definition of "confidential journalistic material" in the IC Code of Practice was too narrow, as it was limited to material acquired for the purpose of journalism and held subject to an undertaking to hold it in confidence. This definition was inconsistent with the Court's broader definition (for example, in *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, no. 39315/06, § 86, 22 November 2012). Secondly, the regime did not comply with the strict requirements of Article 10 where surveillance measures might reveal journalistic source material (in the applicants' submissions, the existence of an "overriding public interest" and judicial – or at least independent – authorisation).

480. With regard to the Chapter II regime, the applicants complained that the ACD Code failed to recognise that communications data could be privileged, and that the obtaining of communications data which constituted confidential journalistic material was as intrusive as obtaining content, since a single piece of communications data could reveal the identity of a journalist's source, and when aggregated and subjected to modern data-mining technology, it could reveal an enormous range of (journalistically privileged) information. The applicants further complained that in most cases authorisation for the acquisition of communications data was provided by a designated person, who was not sufficiently independent of the executive, or even of the agency requesting the disclosure. While an additional safeguard now existed requiring that applications made in order to identify a journalist's source be authorised by a judge, they did not apply where the identification of the source was incidental rather than intended.

(b) The Government

481. In the Government's submissions, prior authorisation was the only respect in which the applicants contended that the position regarding the "in accordance with the law" test might differ under Article 10 from that under Article 8, and in respect of which they asserted that their identity as journalists might be material to the analysis. However, there was no authority in the Court's case-law for the proposition that prior judicial (or independent) authorisation was required for a strategic monitoring regime by virtue of the fact that some journalistic material might be intercepted in the course of that regime's operation. On the contrary, the Court had drawn a sharp and important distinction between the strategic monitoring of

communications and/or communications data, which might inadvertently "sweep up" some journalistic material, and measures that targeted journalistic material, particularly for the purposes of identifying sources, where prior authorisation would be required.

482. With regard to Chapter II of RIPA, the Government pointed out that pursuant to the amended Acquisition and Disclosure of Communications Data Code of Practice ("the ACD Code"), where the identification of a journalist's source was intended, judicial authorisation was required. As there was nothing "unintentional" about the operation of the Chapter II regime, the acquisition of communications data under it would always be intentional and further safeguards were not required for the unintentional acquisition of material disclosing a journalist's source.

483. The Government further argued that the ACD Code provided for the protection of confidential material, including journalistic material. Such material should only be retained where necessary and proportionate for one of the authorised purposes in section 15(4) of RIPA; it must be destroyed securely when its retention was no longer needed for those purposes; and, if retained, there had to be adequate information management systems in place to ensure that retention remained necessary and proportionate. Where it was retained or disseminated to an outside body, reasonable steps had to be taken to mark it as confidential, and where any doubt existed, legal advice had to be sought about its dissemination. Finally, any case where confidential material was retained had to be notified to the Commissioner as soon as reasonably practical and the material had to be made available to the Commissioner on request.

2. The submissions of the third parties

(a) The Helsinki Foundation for Human Rights

484. The Helsinki Foundation submitted that the protection of journalistic sources was undermined not only by the surveillance of the content of journalists' communications, but also by the surveillance of related metadata which could, by itself, allow for the identification of sources and informants. It was especially problematic that confidential information could be acquired without the journalists' knowledge or control, thereby depriving them of their right to invoke confidentiality, and the ability of their sources to rely on guarantees of confidentiality.

(b) The National Union of Journalists ("NUJ") and the International Federation of Journalists ("IFJ")

485. The NUJ and the IFJ submitted that the confidentiality of sources was indispensable for press freedom. They also expressed concern about the possible sharing of data retained by the United Kingdom with other countries. If confidential journalistic material were to be shared with a

country which could not be trusted to handle it securely, it could end up in the hands of people who would harm the journalist or his or her source. In the interveners' view, the safeguards in the updated IC and ACD Codes of Practice were not adequate, especially where the journalist or the identification of his or her source was not the target of the surveillance measure.

(c) The Media Lawyers' Association ("MLA")

486. The MLA expressed deep concern that domestic law was moving away from the strong presumption that journalistic sources would be afforded special legal protection, since surveillance regimes allowed the authorities to intercept journalists' communications without the need for prior judicial authorisation. Since the protection of journalists' sources was one of the core components of Article 10, more robust protection was required.

3. The Court's assessment

(a) General principles

487. The Court reiterates that freedom of expression constitutes one of the essential foundations of a democratic society and that the safeguards to be afforded to the press are of particular importance. The protection of journalistic sources is one of the cornerstones of freedom of the press. Without such protection, sources may be deterred from assisting the press in informing the public about 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 (see, *inter alia*, *Sanoma Uitgevers B.V.*, cited above, § 50; *Weber and Saravia*, cited above, § 143; *Goodwin*, cited above, § 39; and *Roemen and Schmit v. Luxembourg*, no. 51772/99, § 46, ECHR 2003-IV).

488. The Court has always subjected the safeguards for respect of freedom of expression in cases under Article 10 of the Convention to special scrutiny. Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society, an interference cannot be compatible with Article 10 of the Convention unless it is justified by an overriding requirement in the public interest (*Sanoma Uitgevers B.V.*, cited above, § 51; *Goodwin*, cited above, § 39; *Roemen and Schmit*, cited above, § 46; and *Voskuil v. the Netherlands*, no. 64752/01, § 65, 22 November 2007).

489. The Court has recognised that there is "a fundamental difference" between the authorities ordering a journalist to reveal the identity of his or her sources, and the authorities carrying out searches at a journalist's home and workplace with a view to uncovering his or her sources (compare *Goodwin*, cited above, with *Roemen and Schmit*, cited above, § 57). The

Court considered that the latter, even if unproductive, constituted a more drastic measure than an order to divulge the source's identity, since investigators who raid a journalist's workplace have access to all the documentation held by the journalist (*Roemen and Schmit*, cited above, § 57). However, the Court has also drawn a distinction between searches carried out on journalists' homes and workplaces "with a view to uncovering their sources", and searches carried out for other reasons, such as the obtaining of evidence of an offence committed by a person other than in his or her capacity as a journalist (*Roemen and Schmit*, cited above, § 52). Similarly, in *Weber and Saravia*, the only case in which the Court has considered, *in abstracto*, the Article 10 compliance of a secret surveillance regime on account of the potential for interference with confidential journalistic material, it considered it decisive that the surveillance measures were not aimed at monitoring journalists or uncovering journalistic sources. As such, it found that the interference with freedom of expression could not be characterised as particularly serious (*Weber and Saravia*, cited above, § 151).

(b) The application of the general principles to the present case

(i) The section 8(4) regime

490. With regard to the question of victim status, the Court recalls that in *Weber and Saravia* it expressly recognised that the impugned surveillance regime had interfered with the first applicant's freedom of expression as a journalist (*Weber and Saravia*, cited above, §§ 143-145). In the present case, the applicants in the second of the joined cases are journalists and can similarly claim to be "victims" of an interference with their Article 10 rights by virtue of the operation of the section 8(4) regime.

491. For the reasons set out in respect of the Article 8 complaint, the Court considers that – save for its concerns about the oversight of the selection process and the safeguards applicable to the selection of related communications data (see paragraph 387 above) – the section 8(4) regime was in accordance with the law (see paragraphs 387-388 above). Furthermore, it pursued the legitimate aims of protecting interests of national security, territorial integrity and public safety, and preventing disorder and crime.

492. With regard to "necessity", the Court reiterates that, having regard to the importance of the protection of journalistic sources for the freedom of the press in a democratic society, an interference could not be compatible with Article 10 of the Convention unless it was justified by an overriding requirement in the public interest (*Weber and Saravia*, cited above, § 149). In this regard, it notes that the surveillance measures under the section 8(4) regime – like those under the G10 Act which were considered in *Weber and Saravia* – are not aimed at monitoring journalists or uncovering journalistic

sources. Generally the authorities would only know when examining the intercepted communications if a journalist's communications had been intercepted. Consequently, it confirms that the interception of such communications could not, by itself, be characterised as a particularly serious interference with freedom of expression (*Weber and Saravia*, cited above, § 151). However, the interference will be greater should these communications be selected for examination and, in the Court's view, will only be "justified by an overriding requirement in the public interest" if accompanied by sufficient safeguards relating both to the circumstances in which they may be selected intentionally for examination, and to the protection of confidentiality where they have been selected, either intentionally or otherwise, for examination.

493. In this regard, paragraphs 4.1 – 4.8 of the IC Code require special consideration to be given to the interception of communications that involve confidential journalistic material and confidential personal information (see paragraph 90 above). However, these provisions appear to relate solely to the decision to issue an interception warrant. Therefore, while they might provide adequate safeguards in respect of a targeted warrant under section 8(1) of RIPA, they do not appear to have any meaning in relation to a bulk interception regime. Furthermore, the Court has already criticised the lack of transparency and oversight of the criteria for searching and selecting communications for examination (see paragraphs 339, 340, 345 and 387 above). In the Article 10 context, it is of particular concern that there are no requirements – at least, no "above the waterline" requirements – either circumscribing the intelligence services' power to search for confidential journalistic or other material (for example, by using a journalist's email address as a selector), or requiring analysts, in selecting material for examination, to give any particular consideration to whether such material is or may be involved. Consequently, it would appear that analysts could search and examine without restriction both the content and the related communications data of these intercepted communications.

494. Safeguards do exist in respect of the storing of confidential material once identified. For example, paragraph 4.29 of the IC Code (see paragraph 90 above) provides that such material should only be retained where it is necessary and proportionate for one of the authorised purposes in section 15(4) of RIPA, and it must be destroyed securely when it is no longer needed for one of these purposes. Furthermore, according to paragraph 4.30, if it is retained or disseminated to an outside body, reasonable steps should be taken to mark the information as confidential; and paragraph 4.31 requires that the Interception of Communications Commissioner be notified of the retention of such material as soon as reasonably practicable, and such material should be made available to him on request.

495. Nevertheless, in view of the potential chilling effect that any perceived interference with the confidentiality of their communications and, in particular, their sources might have on the freedom of the press and, in the absence of any "above the waterline" arrangements limiting the intelligence services' ability to search and examine such material other than where "it is justified by an overriding requirement in the public interest", the Court finds that there has also been a violation of Article 10 of the Convention.

(ii) The Chapter II regime

496. The applicants in the second of the joined cases also complained under Article 10 of the Convention about the regime for the acquisition of communications data from CSPs.

497. In considering the applicants' Article 8 complaint, the Court concluded that the Chapter II regime was not in accordance with the law as it permitted access to retained data for the purpose of combating crime (rather than "serious crime") and, save for where access was sought for the purpose of determining a journalist's source, it was not subject to prior review by a court or independent administrative body (see paragraph 467 above).

498. The Court acknowledges that the Chapter II regime affords enhanced protection where data is sought for the purpose of identifying a journalist's source, In particular, paragraph 3.77 of the ACD Code provides that where an application is intended to determine the source of journalistic information, there must be an overriding requirement in the public interest, and such applications must use the procedures of the Police and Criminal Evidence Act 1984 ("PACE") to apply to a court for a production order to obtain this data (see paragraph 117 above). Pursuant to Schedule 1 to PACE, an application for a production order is made to a judge and, where the application relates to material that consists of or includes journalistic material, the application should be made *inter partes* (see paragraph 121 above). The internal authorisation process may only be used if there is believed to be an immediate threat of loss of human life, and that person's life might be endangered by the delay inherent in the process of judicial authorisation (paragraphs 3.76 and 3.78-3.84 of the ACD Code – see paragraph 117 above).

499. Nevertheless, these provisions only apply where the purpose of the application is to determine a source; they do not, therefore, apply in every case where there is a request for the communications data of a journalist, or where such collateral intrusion is likely. Furthermore, in cases concerning access to a journalist's communications data there are no special provisions restricting access to the purpose of combating "serious crime". Consequently, the Court considers that the regime cannot be "in accordance with the law" for the purpose of the Article 10 complaint.

(iii) Overall conclusion

500. In respect of the complaints under Article 10 of the Convention, the Court therefore finds a violation in respect of the section 8(4) regime and the Chapter II regime.

IV. ALLEGED VIOLATION OF ARTICLE 6 OF THE CONVENTION

501. The applicants in the third of the joined cases further complained under Article 6 of the Convention that the limitations inherent in the IPT proceedings were disproportionate and impaired the very essence of their right to a fair trial.

502. Article 6 provides, as relevant:

> "1. In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice."

503. In particular, the applicants contended that there was a lack of independence and impartiality on the part of the IPT, evidenced by the fact that in November 2007 there had been a secret meeting between it and the Security Services which, they alleged, resulted in the adoption of a protocol pursuant to which MI5 agreed not to search or disclose any bulk data holdings relating to complainants; that they were not effectively represented in the closed proceedings; that the IPT failed to require the defendants to disclose key internal guidance; and that, following the hearing, the IPT had made its determination in favour of the wrong party.

504. The Government submitted that Article 6 of the Convention did not apply to surveillance proceedings, since the Commission and the Court had consistently held that decisions authorising surveillance did not involve the determination of "civil rights and obligations" within the meaning of Article 6 § 1. They further contended that even if Article 6 did apply, when the proceedings were taken as a whole the applicants could not be said to have been denied the right to a fair trial. In particular, they observed that the applicants did not have to overcome any evidential burden to apply to the IPT; there was scrutiny of all the relevant material, open and closed, by the IPT, which had full powers to obtain any material it considered necessary; material was only withheld where the IPT was satisfied that there were appropriate public interest and national security reasons for doing so; and finally, the IPT appointed Counsel to the Tribunal who in practice performed a similar function to that of a Special Advocate in closed material proceedings. With regard to the meeting in 2007 between MI5 and the IPT,

they advised the Court that at the meeting MI5 had indicated that, for the purposes of IPT proceedings, it would not routinely conduct searches of "reference data-bases", being databases containing information about the population generally (such as the Voter's Roll or telephone directories), for any mention of a complainant's name; instead, such searches would only be carried out if the data was "relevant or had been relied on in the course of an investigation".

505. In their third party intervention, the ENNHRI submitted that the principle of equality of arms – being a core aspect of Article 6 of the Convention – was incompatible with the exclusion of one party from a hearing in which the other participates, other than in exceptional circumstances where adequate procedural safeguards provide protection from unfairness and no disadvantage ensues.

506. To date, neither the Commission nor the Court has found that Article 6 § 1 of the Convention applies to proceedings relating to a decision to place a person under surveillance. For example, in *Klass v. Germany* the Commission found that Article 6 § 1 was not applicable either under its civil or under its criminal limb (see *Klass and Others*, cited above, §§ 57-61) and, more recently, in *Association for European Integration and Human Rights and Ekimdzhiev* (cited above, § 106) the Court "did not perceive anything in the circumstances of the case that could alter that conclusion".

507. However, the IPT has itself gone further than this Court. In its joint Ruling on Preliminary Issues of Law in the *British-Irish Rights Watch Case*, it accepted that Article 6 applied to "a person's claims under section 65(2)(a) and to his complaints under section 65(2)(b) of RIPA, as each of them involves "the determination of his civil rights' by the Tribunal within the meaning of Article 6(1)" (see paragraph 137 above). Consequently, when the matter came before the Court in *Kennedy* it did not consider it necessary to reach a conclusion on the matter, since it held that, even assuming that Article 6 § 1 applied to the proceedings in question, there had been no violation of that Article (*Kennedy*, cited above, §§ 177-179 and §§ 184-191).

508. In the present case, it is similarly unnecessary for the Court to reach any firm conclusion on the question of the applicability of Article 6 of the Convention since, for the reasons set out below, it considers that the applicants' complaint is manifestly ill-founded.

509. With regard to the applicants' general complaints concerning the procedure before the IPT, including the limitations on disclosure and the holding of public hearings in the interests of national security, the Court recalls that similar complaints were made in *Kennedy* and the Court, having considered the relevant procedural rules, concluded that 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 restrictions on the applicant's procedural rights were both

necessary and proportionate and did not impair the very essence of his Article 6 rights (*Kennedy*, cited above, §§ 177-179 and §§ 184-191).

510. The Court sees no reason to come to a different conclusion in the present case. It has already found, in paragraphs 250-265 above, that in view of the IPT's extensive power to consider complaints concerning the wrongful interference with communications pursuant to RIPA, it was an effective remedy, available in theory and practice, which was capable of offering redress to persons complaining of both specific incidences of surveillance and the general Convention compliance of a surveillance regime. Furthermore, these extensive powers were employed in the applicants' case to ensure the fairness of the proceedings; in particular, there was scrutiny of all the relevant material, open and closed, by the IPT; material was only withheld from the applicants where the IPT was satisfied that there were appropriate public interest and national security reasons for doing so; and finally, the IPT appointed Counsel to the Tribunal to make submissions on behalf of the applicants in the closed proceedings.

511. Insofar as the applicants complain about the meeting between the IPT and the intelligence services in 2007, the Court considers that, in view of the IPT's specialist role, the fact that its members met with the services to discuss procedural matters does not, of itself, call into question its independence and impartiality. Furthermore, the applicants have not adequately explained how the 2007 meeting impacted on the fairness of their IPT proceedings in 2014 and 2015. Although the applicants appear to suggest that the resulting protocol might have affected the IPT's ability to access information held about them, the Government's explanation of the protocol (namely, that it concerned an agreement not to conduct searches of databases containing information about the population generally, such as the Voter's Roll or telephone directories, unless the data was "relevant or had been relied on in the course of an investigation") confirms that it could have had no impact on the fairness of the IPT proceedings in the present case.

512. Finally, it would appear that the error regarding the identity of the applicants whose rights were violated was an administrative mistake (see paragraph 53 above) and, as such, does not indicate any lack of rigour in the judicial process.

513. Accordingly, the Court considers that the complaint under Article 6 § 1 of the Convention must be rejected as manifestly ill-founded pursuant to Article 35 § 3 (a) of the Convention.

V. ALLEGED VIOLATION OF ARTICLE 14 OF THE CONVENTION COMBINED WITH ARTICLES 8 AND 10 OF THE CONVENTION

514. The applicants in the third of the joined cases further complained under Article 14 of the Convention, read together with Articles 8 and 10, that the section 8(4) regime was indirectly discriminatory on grounds of

nationality because persons outside the United Kingdom were disproportionately likely to have their private communications intercepted; and section 16 of RIPA provides additional safeguards only to persons known to be in the British Islands.

515. Article 14 provides as follows:

> "The enjoyment of the rights and freedoms set forth in [the] Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status."

516. However, the applicants have not substantiated their claim that persons outside the United Kingdom are disproportionately likely to have their private communications intercepted under the section 8(4) regime. First of all, although the regime targets "external communications", this is defined as "a communication sent or received outside the British Islands". This does not, therefore, exclude the interception of communications where one of the parties is in the British Islands. Secondly, and in any event, it has already been acknowledged that "internal communications" (where both the sender and receiver are in the British Islands) are frequently – and lawfully – intercepted as a by-catch of a section 8 (4) warrant.

517. Insofar as section 16 prevents intercepted material from being selected for examination according to a factor "referable to an individual who is known to be for the time being in the British Islands", any resulting difference in treatment would not be based directly on nationality or national origin, but rather on geographical location. In *Magee v. the United Kingdom*, no. 28135/95, § 50, ECHR 2000-VI the Court held that as such a difference in treatment could not be explained in terms of personal characteristics, it was not a relevant difference in treatment for the purposes of Article 14 of the Convention and did not amount to discriminatory treatment within the meaning of Article 14 of the Convention (see *Magee*, cited above, § 50).

518. In any event, the Court is of the view that any difference in treatment based on geographic location was justified. The Government have considerable powers and resources to investigate persons within the British Islands and do not have to resort to interception of their communications under a section 8(4) warrant. They do not, however, have the same powers to investigate persons outside of the British Islands.

519. Accordingly, the Court considers that the complaint under Article 14 of the Convention, read together with Articles 8 and 10, must be rejected as manifestly ill-founded pursuant to Article 35 § 3(a) of the Convention.

VI. APPLICATION OF ARTICLE 41 OF THE CONVENTION

520. Article 41 of the Convention provides:

> "If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

A. Damage

521. The applicants did not submit any claim in respect of pecuniary or non-pecuniary damage. Accordingly, the Court considers that there is no call to award them any sum on that account.

B. Costs and expenses

522. The applicants in the first and second of the joined cases made a claim for costs and expenses incurred before the Court. The applicants in the first of the joined cases claimed GBP 208,958.55 in respect of their costs and expenses; and the applicants in the second of the joined cases claimed GBP 45,127.89. The applicants in the third of the joined cases made no claim in respect of costs and expenses.

523. The Government did not comment on the sums claimed.

524. According to the Court's case-law, an applicant is entitled to the reimbursement of costs and expenses only in so far as it has been shown that these have been actually and necessarily incurred and are reasonable as to quantum. In the present case, regard being had to the documents in its possession and the above criteria, the Court considers it reasonable to award the applicants in the first of the joined cases the sum of EUR 150,000 for the proceedings before the Court; and the applicants in the second of the joined cases the sum of EUR 35,000 for the proceedings before the Court.

C. Default interest

525. The Court considers it appropriate that the default interest rate should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

FOR THESE REASONS, THE COURT:

1. *Declares*, unanimously, the complaints made by the applicants in the third of the joined cases concerning Article 6, Article 10, insofar as the applicants rely on their status as NGOs, and Article 14 inadmissible;

2. *Declares*, unanimously, the remainder of the complaints made by the applicants in the third of the joined cases admissible;

3. *Declares*, by a majority, the complaints made by the applicants in the first and second of the joined cases admissible;

4. *Holds*, by five votes to two, that there has been a violation of Article 8 of the Convention in respect of the section 8(4) regime;

5. *Holds*, by six votes to one, that there has been a violation of Article 8 of the Convention in respect of the Chapter II regime,

6. *Holds*, by five votes to two, that there has been no violation of Article 8 of the Convention in respect of the intelligence sharing regime;

7. *Holds*, by six votes to one, that, insofar as it was raised by the applicants in the second of the joined cases, there has been a violation of Article 10 of the Convention in respect of the section 8(4) regime and the Chapter II regime;

8. *Holds*, unanimously, that there is no need to examine the remaining complaints made by the applicants in the third of the joined cases under Article 10 of the Convention;

9. *Holds*, by six votes to one,
   (a) that the respondent State is to pay the applicants, within three months from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, the following amounts, to be converted into the currency of the respondent State at the rate applicable at the date of settlement:
      (i) to the applicants in the first of the joined cases: EUR 150,000 (one hundred and fifty thousand euros), plus any tax that may be chargeable to the applicants, in respect of costs and expenses;
      (ii) to the applicants in the second of the joined cases: EUR 35,000 (thirty-five thousand euros), plus any tax that may be chargeable to the applicants, in respect of costs and expenses;
   (b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amounts at a

rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points; and

10. *Dismisses*, unanimously, the remainder of the applicants' claim for just satisfaction.

Done in English, and notified in writing on 13 September 2018, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Abel Campos Registrar	Linos-Alexandre Sicilianos President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the following separate opinions are annexed to this judgment:

(a) partly concurring, partly dissenting opinion of Judge Koskelo, joined by Judge Turković; and

(b) joint partly dissenting and partly concurring opinion of Judges Pardalos and Eicke.

L.-A.S.
A.C.

APPENDIX

List of Applicants

App. No.	Applicants
58170/13	Big Brother Watch
58170/13	English PEN
58170/13	Open Rights Group
58170/13	Dr Constanze Kurz
62322/14	Bureau of Investigative Journalism
62322/14	Alice Ross
24960/15	Amnesty International Limited
24960/15	Bytes For All
24960/15	The National Council for Civil Liberties (“Liberty”)
24960/15	Privacy International
24960/15	The American Civil Liberties Union
24960/15	The Canadian Civil Liberties Association
24960/15	The Egyptian Initiative For Personal Rights
24960/15	The Hungarian Civil Liberties Union
24960/15	The Irish Council For Civil Liberties Limited
24960/15	The Legal Resources Centre

PARTLY CONCURRING, PARTLY DISSENTING OPINION OF JUDGE KOSKELO, JOINED BY JUDGE TURKOVIĆ

1. I have voted, and agree, with the majority as regards points 1 to 3 of the operative provisions of the judgment, which concern the admissibility of the complaints. I have also joined the majority in finding a violation of Article 8 in respect of both the section 8(4) regime and the Chapter II regime. As regards the section 8(4) regime, however, I am not able in all respects to subscribe to the reasons given by the majority. As far as the intelligence sharing regime is concerned, unlike the majority, I have voted for finding a violation of Article 8.

I. The RIPA section 8(4) regime

2. The present case concerns legislation providing for secret surveillance, by means of bulk interception, of electronic communications which qualify as "external" (for an understanding of the concept of "external" communications see paragraphs 69-71 of the judgment). It is important to note that this type of secret surveillance of communications is not limited to certain already known or identified targets but is aimed at the discovery of threats and hitherto unknown or unidentified targets which might be responsible for threats (see paragraph 284 of the judgment). The relevant threats are broadly framed and comprise threats to national security or to the economic well-being of the country as well as threats arising from serious crime (see §§ 57-59).

3. It is obvious that such an activity – an untargeted surveillance of external communications with a view to discovering and exploring a wide range of threats – by its very nature takes on a potentially vast scope, and involves enormous risks of abuse. The safeguards against those risks, and the standards which under the Convention should apply in this regard, therefore raise questions of the highest importance. I am not convinced, in the light of present-day circumstances, that reliance on the Court's existing case-law provides an adequate approach to the kind of surveillance regimes like the one we are dealing with here. A more thorough reconsideration would be called for. I acknowledge that this would be a task for the Court's Grand Chamber. I will only raise some concerns which, in my view, require attention in this regard.

(i) The context of earlier case-law

4. Apart from the recent Chamber judgment in *Centrum för Rättvisa v. Sweden* (no. 35252/08, 19 June 2018), which is not yet final, the Court's case-law has not dealt with the present kind of surveillance but with regimes which, as a matter of either law or fact, have been narrower in scope. Furthermore, in the light of current developments, I consider that reliance

on the line of existing case-law is no longer an adequate basis for assessing the standards which under the Convention should govern this particular domain.

5. The Court's case-law on secret surveillance of communications essentially dates back to *Klass and Others v. Germany* (cited in the judgment) which was decided by the Plenary Court four decades ago, and the admissibility decision in *Weber and Saravia v. Germany* (also cited in the judgment), which concerned an amended version of the same German legislation and was decided twelve years ago, in response to a complaint lodged in the year 2000.

6. As the Court noted in *Klass and Others*, the German legislation then at issue (the G 10) laid down a series of limitative conditions which had to be satisfied before a surveillance measure could be imposed. Thus, the permissible restrictive measures were *confined to cases in which there were factual indications for suspecting a person of planning, committing or having committed certain serious criminal acts*; measures could only be ordered if the establishment of the facts by another method was without any prospect of success or considerably more difficult; even then, the surveillance could cover *only the specific suspect or his presumed "contact-persons"*. Thus, the Court observed, "*so-called exploratory or general surveillance [was] not permitted by the contested legislation*" (see *Klass and Others*, § 51).

7. In this regard, the RIPA section 8(4) regime which is at issue in the present case is different from that in *Klass and Others* in that the section 8(4) regime does encompass what the Court then referred to as "exploratory" surveillance and which in fact constitutes an essential and critical feature of this particular regime. Consequently, the scope and purpose of the surveillance regime now at issue is wider than that addressed in *Klass and Others*.

8. In *Weber and Saravia*, the complaint concerned a revised version, adopted in 1994, of the German G 10, whereby the scope of permissible surveillance was extended to cover the monitoring of international wireless telecommunications (see *Weber and Saravia*, § 88) in order to allow a "strategic surveillance" of such communications by means of catchwords. According to the Government's submissions in that case, at the relevant time merely some ten per cent of all telecommunications were conducted by wireless means, and thus potentially subject to monitoring. In practice, monitoring was restricted to a limited number of foreign countries. The telephone connections of the State's own (i.e. German) nationals living abroad could not be monitored directly. The identity of persons telecommunicating could only be uncovered in rare cases in which a catchword had been used (ibid., § 110).

9. The surveillance regime at issue in *Weber and Saravia* covered international wireless communications traffic, i.e. traffic transmitted via

microwave or satellite, the latter operating through a survey of the downlink to Germany. Line-bound international communications were not subject to monitoring except where the risk of a war of aggression was concerned.

10. It is noteworthy that at the time of the surveillance regime which gave rise to the complaint in *Weber and Saravia*, strategic monitoring was mainly carried out on telephone, telex and fax communications. In those days, surveillance did not extend to email communications (see the judgment of the Federal Constitutional Court of 14 July 1999, 1BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95, Rn 230, according to which, at the time of the hearing of the case in 1999, an expansion of strategic monitoring to email communications was only being planned for the future). One significant feature of communications by email, apart from the fact that nowadays they are so common, is that the identity of both the sender and recipient is usually directly available. Furthermore, many currently used means of communication or access to information through the Internet were only at embryonic stages at the time of the domestic complaint in *Weber and Saravia*.

(ii) The context of the present case

11. My point with the remarks above is to draw attention to the factual environment against the background of which those earlier cases were adjudicated, and the dramatic changes that have occurred since. The applicants have indeed referred to the technological "sea change" which has taken place.

12. What is important to note in this regard is that the technological "sea change" has had a twofold impact. On the one hand, technological developments have advanced the means by which surveillance of communications can be carried out. On the other hand, new technologies have revolutionised the ways in which people communicate, access, use and share information. That change is deeper than just a matter of volume. The digital age has in some respects transformed people's lifestyles.

13. As a result of these changes, the potential exposure nowadays of a vast range of communications and other online activities to secret surveillance is far greater than before. In the wake of such developments, the potential risks of abuse arising from such surveillance have increased as well. Thus, the factual context in which "exploratory" or "strategic" secret surveillance operates is dramatically different from the circumstances that still prevailed a couple of decades ago, when the *Weber and Saravia* application was lodged, let alone four decades ago, when *Klass and Others* was decided. In the light of such changes, it is problematic and troubling to approach the question of the necessary safeguards against abuse simply by applying standards that were considered sufficient under significantly or even essentially different factual circumstances.

14. Furthermore, the "sea change" in terms of technologies and digitalised lifestyles is not the only development to be taken into consideration. The threats on account of which surveillance of communications is considered necessary have also changed. In this regard, too, the picture is twofold. One the one hand, for instance, there have been real and well-known aggravations in the risks of international terrorism. On the other, there is also increasing evidence of how various threats can be invoked, rightly or wrongly, in order to justify measures that entail restrictions on individual rights and freedoms. The notion of terrorism, for instance, may sometimes be used quite loosely and opportunistically in a desire to legitimise interferences with such rights and freedoms. Especially where secret surveillance is conducted in order to discover and explore broadly formulated threats such as those to national security or the nation's economic well-being, the need for real safeguards through independent control and review is obvious.

15. There is yet another "sea change" calling for heightened attention in the assessment of the necessary standards in the context of secret surveillance of communications. It is the degradation of respect for democratic standards and the rule of law of which there is increasing evidence in a number of States. While I am not suggesting that the present respondent State is a case in point in this regard, the Convention standards must nevertheless be considered in the light of the fact that such developments testify to the actual or potential fragility of safeguards, institutional arrangements and the underlying assumptions that in ideal circumstances might appear adequate in order to minimise the risks of abuse. In fact, the same threats that are invoked to justify secret surveillance may also serve to reinforce tendencies toward a weakening of the checks and balances which underpin adherence to the rule of law and democratic governance.

(iii) Concerns

16. In line with the majority, I agree that the Contracting States must enjoy a wide margin of appreciation in determining whether the protection of national security requires the kind of surveillance of communications which is at issue in the present case (paragraph 314 of the present judgment). However, given the high risks of abuse, which at worst may undermine not only individual rights and freedoms but democracy and the rule of law more generally, the margin must be narrow when it comes to the necessary safeguards against abuse.

17. Under the impugned legislation, one of the striking features is that all of the supervisory powers entrusted to authorities with independence from the executive are of an *ex post* nature. Another striking feature is that not only are the general protective aims of the legislation very broadly framed, but also the specific authorisations (warrants and certificates) issued

by the Secretary of State appear to be formulated in very broad and general terms (see paragraphs 156 and 342). Furthermore, the concrete search and selection criteria which are applied to filter intercepted communications for reading of their content are determined by the analysts conducting the surveillance (see paragraphs 157, 340 and 345-46 of the present judgment). As indicated by the domestic findings, the latter are not even subject to any meaningful subsequent oversight by independent bodies (see paragraphs 157 and 340).

18. Ever since *Klass and Others*, the Court has indeed held that in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse (see *Klass and Others*, §§ 49-50). This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the 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 (ibid., § 50).

19. As discussed above, in the light of the changes in both the nature and scope of surveillance and in the prevailing factual realities, the circumstances have indeed evolved in such a way and to such an extent that I find it difficult to accept that the adequacy of safeguards should nevertheless be assessed simply by relying on the case-law that has arisen under different legal and factual framework conditions.

20. In particular, given the present overall context, I question the approach according to which prior independent control by a judicial authority should not be a necessary requirement in the system of safeguards.

21. Already in *Klass and Others*, when considering the initial stage of control, the Court stated that, in a field where abuse was potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it was in principle desirable to entrust supervisory control to a judge (see *Klass and Others*, § 56). Under the G 10 legislation, judicial control was replaced by an initial control effected by an official qualified for judicial office and by the control provided by the Parliamentary Board and the G 10 Commission. In that case the Court concluded that, having regard to the nature of the supervisory and other safeguards provided for by the G 10, the exclusion of judicial control did not exceed the limits of what might be deemed necessary in a democratic society. The Court noted that the Parliamentary Board and the G 10 Commission were independent of the authorities carrying out the surveillance and vested with sufficient powers and competence to exercise an effective and continuous control. Furthermore, the democratic character was reflected in the balanced membership of the Parliamentary Board, on which the opposition was represented and was thus able to participate in the

control of the measures ordered by the competent Minister, who was accountable to the Bundestag. The Court found that the two supervisory bodies could, in the circumstances of the case, be regarded as enjoying sufficient independence to give an objective ruling (ibid.).

22. As indicated above, in my view the legal and factual circumstances of that case, which go back four decades, cannot be considered comparable to the situation now under consideration. It is somewhat striking that in *Weber*, despite the important changes in the legislative and factual framework, the Court succinctly stated that it saw no reason to reconsider the conclusion in *Klass and Others* (see *Weber and Saravia*, § 117). In any event, in the light of the circumstances prevailing at the present time, such reconsideration seems to me to be indispensable.

23. Where, as in the present case, the interception (as a matter of technical necessity) encompasses vast volumes of communications traffic in an indiscriminate manner, without being linked to any kind of prior elements of suspicion related to the threats by reason of which the surveillance is conducted, everything in terms of the protection of individuals and their rights depends on whether and how the subsequent stages of the treatment of the intercepted communications provide effective and reliable safeguards for those rights, and against any abuse of the surveillance. Under such circumstances, given the potential intrusiveness of the surveillance and the abundant risks of abuse, I consider that it cannot be appropriate that all the *ex ante* safeguards remain in the hands of the executive. I think the applicants are right to argue that there is a need for an "updating" of the standards as regards prior independent judicial authorisation. It seems to me to be important that the authorities of the executive branch should be required to explain and justify before an independent judicial authority the grounds on which a particular surveillance should be authorised, and to account for the search criteria on the basis of which the intercepted communications will be filtered and selected for a review of their content.

24. In this respect, I am not convinced by the arguments advanced by the majority in support of the position that prior judicial control is unnecessary (paragraphs 318-20). The majority acknowledge that judicial authorisation is not inherently incompatible with the effective functioning of bulk interception (paragraph 318). Indeed, the recent case of *Centrum för Rättvisa v. Sweden* (cited above) offers an illustration, as it deals with Swedish legislation under which prior judicial authorisation is required.

25. The main argument against imposing such a requirement appears to be that it would not entail a sufficient safeguard, and that even in the absence of prior judicial authorisation the existence of independent oversight by the IPT and the Interception of Communications Commissioner provide adequate safeguards against abuse. In my view, it is obvious that prior judicial authorisation cannot in itself be sufficient and

that further, robust safeguards such as those in place in the UK are indeed required. However, the fact that a given safeguard would not be sufficient is not enough to support a conclusion that it should not be considered necessary. In my opinion, it is quite essential to have in place an adequate system of safeguards, including controls exercised by independent bodies, both *ex ante* and *ex post*.

26. While the safeguards *ex post* that are provided for in the UK legislation and practice appear to set a good model in this domain, this does not in my view suffice to remedy the fact that the authorisation and implementation of the surveillance are wholly in the hands of the executive authorities, without any independent control *ex ante*. In this respect, the system of safeguards is even weaker than that considered by the Court in both *Klass and Others* and *Weber and Saravia*, in that under the German G 10 regime, although the surveillance was not subject to prior authorisation by a court, it had to be authorised by the G 10 Commission (see *Weber and Saravia*, cited above, § 115), which was not an executive branch body (ibid., § 25). Moreover, according to the judgment of the Federal Constitutional Court of 14 July 1999 (cited above, Rn 87), a list of search concepts was part of each restriction order, whereas in the present case it has transpired that the search and selection criteria are determined by the analysts operating the surveillance and are not subject to any prior supervision, nor any meaningful subsequent oversight (see paragraphs 157, 340 and 345-46 of the present judgment).

27. In sum, what we have before us now is a regime of secret surveillance, the reach of which under the prevailing factual circumstances is unprecedented, and under which a very wide operational latitude is left to the services operating the surveillance, without any independent *ex ante* control or constraint, and under which the search and selection criteria are not even *ex post* subject to any robust independent control. I find such a situation highly problematic. An independent *ex ante* control is all the more important because of the secret nature of the surveillance, which in practice reduces the possibility that individuals will have recourse to the safeguards available *ex post*.

28. I also consider that the remarks made by the majority in paragraph 319 of the judgment are not capable of supporting a conclusion according to which prior independent judicial authorisation should not be required. Rather, the argument that even judicial scrutiny may fail its function serves to underline the crucial importance which attaches to the requirement that such control must have effective guarantees of independence, in order to meet the proper standards of the necessary safeguards.

29. In short, while I agree with the conclusions set out in paragraph 387 of the judgment, I do not consider those shortcomings to be the only ones that justify a finding of a violation of Article 8 in the present case. In

particular, taking into account the present legal and factual context, I do not believe that the necessary safeguards in the circumstances of surveillance based on the bulk interception of communications can be sufficient without including an independent *ex ante* judicial control. The position according to which prior judicial control of authorisations for secret surveillance of communications was a desirable but not a necessary safeguard stems from *Klass and Others* which, firstly, concerned a more limited surveillance regime than the one now at issue and did not permit "exploratory surveillance" at all, and which, secondly, was decided four decades ago against the backdrop of factual circumstances that in many relevant respects were different from those prevailing today. That position was later, in *Weber and Saravia*, carried over to a surveillance regime which did have more similarities with the RIPA section 8(4) regime but nevertheless operated in conditions very different from those prevailing in the modern digitalised societies. For the reasons outlined above, that position should, in my view, no longer be maintained by the Court.

II. The intelligence-sharing regime

30. It is easy to agree with the principle that any arrangement under which intelligence from intercepted communications is obtained via foreign intelligence services, whether on the basis of requests to carry out such interception or to convey its results, should not be allowed to entail a circumvention of the safeguards which must be in place for any surveillance by domestic authorities (see paragraphs 216, 423 and 447). Indeed, any other approach would be implausible.

31. On this basis I consider, in sum, that the shortcomings referred to above in the context of the section 8(4) regime also attach to the intelligence-sharing regime (see paragraphs 109 and 428-29). I therefore conclude that the safeguards have not been adequate and that there has been a violation of Article 8 in respect of this regime also.

JOINT PARTLY DISSENTING AND PARTLY CONCURRING OPINION OF JUDGES PARDALOS AND EICKE

Introduction

1. For the reasons set out in more detail below, we are unfortunately, not able to agree with the majority in relation to two aspects of the judgment in this case; namely

(a) that the applicants in the first and second of the joined cases had shown "special circumstances absolving them from the requirement to exhaust" domestic remedies by first bringing proceedings before the IPT (§§ 266-268 and operative part § 3; "admissibility"); and

(b) that there has been a breach of Article 8 of the Convention in respect of the section 8(4) regime (§ 388 and operative part § 4; "the section 8(4) regime").

2. In relation to the latter issue our position is reinforced by the contrast between the conclusions reached by the majority in this case and that reached in the judgment in *Centrum För Rättvisa v. Sweden*, no. 35252/08 (not yet final); a judgment adopted by the Third Section of this Court on 19 June 2018, a mere two weeks before the final deliberations in this case. In that case, the Court concluded, unanimously, that, despite having identified "some areas where there is scope for improvement" (§ 180) and "making an overall assessment and having regard to the margin of appreciation enjoyed by the national authorities in protecting national security" (§ 181), the Swedish system of signals intelligence provided adequate and sufficient guarantees against arbitrariness and the risk of abuse; as a consequence, it was held that the relevant legislation met the "quality of law" requirement, that the "interference" established could be considered as being "necessary in a democratic society" and that the structure and operation of the system were proportionate to the aim sought to be achieved.

3. That said, we agree both with:

(a) the underlying general principles identified by the Court both in this case and in *Centrum För Rättvisa* to be applied in relation to these aspects of the case; as well as

(b) the conclusion of the majority in this case that, for the reasons given in the judgment, there has been no breach of Article 8 of the Convention in relation to the intelligence sharing regime (§§ 447-448 and operative part § 6) and that there is no need to examine the remaining complaints made by the applicants in the third of the joined cases under Article 10 of the Convention.

4. In relation to the findings that there has been a breach of the Convention in relation to the Chapter II regime (§§ 468 and 500, operative part §§ 5 and 7) as well as the conclusions under Article 41 of the Convention (operative part § 9), one of us (Judge Pardalos) considered that her conclusion on the admissibility of the first and second of the joined cases invariably determined the related substantive issues against the applicants in those cases. By contrast, Judge Eicke considered that, the Court having decided that the first and second cases were, contrary to his view, admissible he was required, as a member of that Court, to go on and decide those cases on the merits by reference to the evidence and pleadings before the Court.

Admissibility

5. As indicated above, we agree with the majority that, for the reasons they give, the IPT is and has been an effective remedy "since Kennedy was decided in 2010" (§ 268); i.e. a remedy which is "available in theory and practice" and "capable of offering redress to applicants complaining of both specific incidences of surveillance and the general Convention compliance of surveillance regimes" (§ 265). Consequently, applicants before this Court will be expected to have exhausted this domestic remedy before the Court has jurisdiction to entertain their application under Article 35 § 1 of the Convention.

6. In addition to the purely legal point that, under Article 35 § 1, the Court "may only deal with the matter after all domestic remedies have been exhausted", we would underline what the majority says in § 256 about the invaluable assistance derived by the Court, in examining a complaint before it, from the "elucidatory" role played by the domestic courts (in this case the IPT) both generally as well as in the specific context of considering the compliance of a secret surveillance regime with the Convention.

7. For the reasons set out below, however, we disagree with the conclusion reached by the majority (§ 268) that there existed, in this case, "special circumstances" absolving the applicants in the first and second of the joined cases from satisfying this requirement.

8. Firstly, as the majority implicitly accepts (§ 267), the case of *Kennedy* is clearly distinguishable on its facts from the present case. After all, the applicant in that case had already brought a specific complaint about the section 8(1) regime before the IPT before applying to this Court. Consequently, unlike the applicants in the first and second of these joined cases, Mr Kennedy was not inviting the Court to consider his general complaint entirely *in abstracto*. Furthermore, in its judgment in that case, the Court considered it "important" that his challenge was (consequently) exclusively a challenge to primary legislation. By contrast, in the present cases the scope of each of the regimes complained of (bulk interception,

intelligence sharing and the acquisition of communications data) is significantly broader than that of the section 8(1) regime, and the applicants' complaints concern not only primary legislation, but the overall legal framework governing those regimes (including the alleged absence of any relevant arrangements or other safeguards). Consideration of the broader legal framework necessarily requires an examination of both RIPA and the relevant Codes of Practice, together with any "below the waterline" arrangements and/or safeguards. In view of the much broader scope of both their complaints and the impugned regimes, none of which had been the subject of any examination by the IPT, it should have been evident to the applicants in the first and second of the joined cases – who were, at all times, represented by experienced counsel – that, unlike *Kennedy*, this was a case in which the general operation of these regimes required further elucidation, and in which the IPT, on account if its "extensive powers ... to investigate complaints before it and to access confidential information" would have been capable of providing a remedy.

9. There is, therefore, also no basis for any suggestion that our approach seeks, in any way, to overturn or "disapply" the Court's unanimous ruling in *Kennedy*. The simple fact is that, in our view, the two are clearly and obviously distinguishable.

10. Secondly, the first applicant, was clearly informed by the Government, in their response to the letter before action of 26 July 2013 (§ 19), that their complaints could be raised in the IPT, a court established specifically to hear allegations by citizens of wrongful interference with their communications as a result of conduct covered by that Act and a court endowed with exclusive jurisdiction to investigate any complaint that a person's communications have been intercepted and, where interception has occurred, to examine the authority for such interception. This letter was, of course, sent at around the same time as the ten human rights organisations which are the applicants in the third of the joined cases, no doubt recognising the need to have exhausted existing effective domestic remedies before applying to this Court, lodged their complaints before the IPT (June to December 2013; § 21). It was also four years after the UK Supreme Court, in its judgment in *R (on the application of A) v B* [2009] UKSC 12, had confirmed the exclusive jurisdiction of the IPT and its ability, as demonstrated by its decisions in *Kennedy* (IPT/01/62 & 77) and *The British-Irish Rights Watch and others v Security Service, GCHQ and the SIS* (IPT/01/77), to adjust the procedures before it as necessary so as to ensure that disputes before it can be determined justly.

11. Thirdly and in any event, even if, contrary to our view, the applicants in the first and second of the joined cases would have been entitled to rely on *Kennedy* at the time they lodged their applications with the Court they nevertheless accepted before this Court (§ 241), by reference to the judgment in *Campbell and Fell v. the United Kingdom*, 28 June 1984,

§§ 62-63, Series A no. 80, that in light of any finding by the Court to the effect that the IPT is an effective remedy, they would now be required to go back and exhaust unless it would be unjust to require them to do so. As these applicants' complaints concern the general operation of the impugned regimes, rather than specific complaints about an interference with their rights under the Convention, they would still be entitled to raise them before the IPT now.

12. Many of the complaints advanced in the first and second of the joined applications (including, in particular, all of those relating to the Chapter II regime, the sharing of non-intercept material with foreign governments and the lack of protection for confidential journalistic material and journalistic sources under the section 8(4) regime) were not addressed in the *Liberty* proceedings and have not yet been determined by the IPT. Consequently, there is no reason to doubt that if the applicants were now to raise those complaints before the IPT, they would have "a reasonable prospect of success". In fact, in respect of the Chapter II complaint it may be thought that they would have a more than reasonable prospect of success. After all, as the majority records in § 463 of the judgment, the Government, in response to a challenge brought by Liberty, recently conceded that Part 4 of the IPA (which included a power to issue "retention notices" to telecommunications operators requiring the retention of data) was incompatible with fundamental rights in EU law: *R (The National Council for Civil Liberties (Liberty)) v Secretary of State for the Home Department & Anor* [2018] EWHC 975 (Admin). As Chapter II of RIPA, like Part 4 of the IPA, permits access to data for the purpose of combating crime (as opposed to "serious crime"), this concession lead the majority to find a violation of Article 8 of the Convention in relation to the Chapter II regime (§ 467) which would suggest that the applicants had a strong basis for challenging, at the domestic level, the compliance of the Chapter II regime with EU law and, indeed, the Convention.

13. The same could not necessarily be said about those complaints raised by the first and/or second of the joined cases which were determined by the IPT in the *Liberty* proceedings; however, those issues were, of course, also raised by the applicants in the third of the joined cases and would therefore (and in fact have been) considered and determined by the Court on its merits.

14. As a result, and in clear contrast with the ultimate conclusion in *Campbell and Fell*, there is here therefore no evidence to suggest that "it would be unjust now to find these complaints inadmissible for failure to exhaust domestic remedies" (*ibid.* at § 63). Consequently, in our view, both the requirements of Article 35 § 5 of the Convention as well as the application of the principle of subsidiarity, in fact, required such a finding.

15. The point made in the judgment about the fundamental importance of the "elucidatory" role of the domestic courts is further underlined by the

complaint made in relation to the Chapter II regime. After all, as the judgment records in § 451, in both their application to the Court and their initial observations, the applicants in the second of the joined cases had incorrectly referred to the Chapter II regime as a regime for the interception of communications data; rather than a regime which permits certain public authorities to acquire communications data from Communications Service Providers ("CSPs"). This "fundamental legal misunderstanding" led the Government to submit *inter alia* that the applicants had put forward no factual basis whatsoever for concluding that their communications were acquired in this way, and that they did not contend that they had been affected, either directly or indirectly, by the regime.

16. As noted above, the Court's conclusion on the Chapter II regime was, of course, ultimately based on the concession by the Government in *R (The National Council for Civil Liberties (Liberty)) v Secretary of State for the Home Department & Anor* [2018] EWHC 975 (Admin) which enabled the majority to find that the equivalent language in the Chapter II regime was "not in accordance with the law" within the meaning of Article 8 of the Convention (§ 467). However, had that not been the case, this Court would have been confronted with the task of considering in detail whether the regime's attendant safeguards were sufficient to satisfy the requirements of the Convention; and that (1) on the basis of a case initially advanced on the basis of a "fundamental legal misunderstanding" about the nature of the regime, (2) without any assistance or findings by the IPT in relation to what the attendant safeguards, both above and below the waterline, in fact were and/or (3) any reasoned conclusion by the IPT as to whether or not they satisfied the requirements of Article 8 (or could be made to satisfy the requirements of Article 8 by means of further disclosure akin to that ordered on 9 October 2014 in the proceedings brought by the applicants in the third of the joined applications). This would plainly have been a wholly undesirable state of affairs.

The section 8(4) regime

17. As indicated above, there is much in the judgment of the majority we agree with.

18. Firstly, we agree with the majority (as well as with the unanimous judgment in *Centrum För Rättvisa*) in relation to the relevant general principles as set out in the judgment. In particular we agree with the affirmation by the majority (as well as the judgment in *Centrum För Rättvisa* and the report by the Venice Commission) that while the Court has considered prior judicial authorisation to be an important safeguard, and perhaps even "best practice", it has also repeatedly confirmed that, by itself, such prior judicial authorisation is neither necessary nor sufficient to ensure compliance with Article 8 of the Convention (§ 320).

19. Secondly, we also agree with the majority in identifying as potential shortcomings (or, to use the language in *Centrum För Rättvisa* "areas where there is scope for improvement") in the operation of the section 8(4) regime "the lack of oversight of the entire selection process, including the selection of bearers for interception, the selectors and search criteria for filtering intercepted communications, and the selection of material for examination by an analyst; and secondly, the absence of any real safeguards applicable to the selection of related communications data for examination" (§ 387).

20. Finally, we agree with the majority as to the correct approach to be applied when considering whether the system under review satisfied the requirement of being "necessary in a democratic society" under Article 8 § 2 of the Convention, namely that:

> "... regard must be had to the actual operation of the system of interception, including the checks and balances on the exercise of power, and the existence or absence of any evidence of actual abuse (see Association for European Integration and Human Rights and Ekimdzhiev, cited above, § 92) (§ 320)
>
> ... it must principally have regard to the actual operation of a system of interception as a whole, including the checks and balances on the exercise of power, and the existence (or absence) of any evidence of actual abuse (...), such as the authorising of secret surveillance measures haphazardly, irregularly or without due and proper consideration (see Roman Zakharov, cited above, § 267) (§ 377)."

21. Where we disagree is (again) in the application of that approach to the system under review.

22. Before setting out in little more detail the basis for our disagreement we note in passing that this Court's underlying approach appears to be in clear contrast to the approach taken by the CJEU in *Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources and Others and Settinger and Others* (Cases C-293/12 and C-594/12) and *Secretary of State for the Home Department v. Watson and Others* (C-698/15). In the former case, the CJEU was considering the validity of the Data Retention Directive, and in the latter, the validity of domestic legislation containing the same provisions as that directive. While its focus was on the retention of data by CSPs, it also considered the question of access to retained data by the national authorities. In doing so, it indicated that access should be limited to what was strictly necessary for the objective pursued and, where that objective was fighting crime, it should be restricted to fighting serious crime. It further suggested that access should be subject to prior review by a court or independent administrative authority, and that there should be a requirement that the data concerned be retained within the European Union. Therefore, while there is some similarity in the language used by the two courts, the CJEU appears to have adopted a more prescriptive approach as regards the safeguards it considers necessary. This may be due to the fact that in both cases it was considering the rights guaranteed by reference to Articles 7 (Respect for private and family life) and 8 (Protection of personal

data) of the Charter of Fundamental Rights. However, while in *Watson* the CJEU declined to state whether the protection provided by Articles 7 and 8 of the Charter was wider than that afforded by Article 8 of the Convention, we can but note that, on the one hand, Article 52 § 3 of the Charter of Fundamental Rights, while recognising the ability of EU law providing more extensive protection, is clearly expressed by reference to "rights" guaranteed by the Convention (rather than "Articles") corresponding to "rights" contained in the Charter and that, on the other hand, this Court has, at least since the 1978 judgment of the Plenary Court in *Klass and Others v. Germany*, Series A no. 28, consistently protected the right to the protection of personal data under Article 8 of the Convention. In any event, in *Ben Faiza v. France*, no. 31446/12, 8 February 2018, which was decided one year after *Watson*, and four years after *Digital Rights Ireland*, this Court did not follow the CJEU's approach, preferring instead to follow its well-established approach and to review the impugned regime as a whole in order to evaluate the adequacy of the available safeguards.

23. In any event, applying this Court's well-established approach, it is in our view, clear from the (in the context of secret surveillance cases unusually) extensive and detailed (publicly available) evidence in relation to the operation of the section 8(4) regime (summarised over some 35 pages in the judgment) that, despite the identified areas where there is scope for improvement, these are not, in themselves, sufficiently significant to justify the conclusion that "the section 8(4) regime does not meet the 'quality of law' requirement and is incapable of keeping the 'interference' to what is 'necessary in a democratic society'" (§ 388). On the contrary, adopting the approach of this Court in *Centrum För Rättvisa*, § 181, it is clear in our view that, making an overall assessment and having regard to the margin of appreciation enjoyed by the national authorities in protecting national security, the section 8(4) regime does provide adequate and sufficient guarantees against arbitrariness and the risk of abuse. As a result, we concluded that the relevant legislation meets the "quality of law" requirement and the "interference" established can be considered as being "necessary in a democratic society" and that there was, therefore, no violation of Article 8 of the Convention.

24. In this context, the contrast to the judgment in *Centrum För Rättvisa* is instructive. After all, in that case the Court applied the same general principles to the Swedish bulk interception regime and concluded, unanimously, that there was no breach of Article 8 of the Convention. Conscious of the difficulty – at times – in making detailed meaningful comparisons between different interception regimes, it is nevertheless noteworthy that the regime under consideration in that case, while equipped with judicial prior authorisation:

(a) was completely shrouded in secrecy with the Court having little meaningful information at all either about the actual generic operation of

the system (including the actual operation of the Foreign Intelligence Court ("FIC") itself) or the impact of the system on and/or operation of safeguards in relation to any individual;

(b) provided that, in principle, the FIC should hold public hearings but found that there has never been a public hearing, all decisions are confidential and no information is disclosed to the public about the number of hearings, the number of permits granted or rejected, the reasoning of the court's decisions or the amount or type of search terms being used. While the FIC is assisted by the "privacy protection representative" whose role it is to protect the "interests of the general public" he or she does not appear on behalf of or represent the interests of any affected individual. Furthermore, the privacy protection representative cannot appeal against a decision by the FIC or "report any perceived irregularities to the supervisory bodies";

(c) was concerned with interception by the National Defence Radio Establishment ("FRA") on behalf of, and which, therefore, required communication of the intercept material to, a much wider group "clients" ("the Government, the Government Offices, the Armed Forces and, as from January 2013, the Security Police and the National Operative Department of the Police Authority");

(d) provided for authorisation of interception for a greater number (eight) of "purposes" ("1) external military threats to the country, 2) conditions for Swedish participation in international peacekeeping or humanitarian missions or threats to the safety of Swedish interests in the performance of such operations, 3) strategic circumstances concerning international terrorism or other serious cross-border crimes that may threaten essential national interests, 4) the development and proliferation of weapons of mass destruction, military equipment and other similar specified products, 5) serious external threats to society's infrastructure, 6) foreign conflicts with consequences for international security, 7) foreign intelligence operations against Swedish interests, and 8) the actions or intentions of a foreign power that are of substantial importance for Swedish foreign, security or defence policy");

(e) had similar difficulties to those identified in relation to the UK regime to separate out non-external communications between a sender and receiver within the respective State at the point of collection;

(f) allows for the communication of intercept product not only to other states but also to "international organisations" (not further defined) where that is "not prevented by secrecy and if necessary for the FRA to perform its activities within international defence and security cooperation" and "it is beneficial for the Swedish government or Sweden's comprehensive defence strategy" and without any provision requiring the third country/international organisation recipient to protect

the data with the same or similar safeguards as those applicable internally; and

(g) provided for an obligation to notify the subject of an intercept after the event; an obligation which, however, "had never been used by the FRA, due to secrecy.

25. Considering the accepted difficulty in making a meaningful comparison between two or more distinct interception regime together with the different conclusions reached by this Court at about the same time, in our view, further underlines the importance of the Court adopting an approach of asking whether, taking "an overall assessment and having regard to the margin of appreciation enjoyed by the national authorities in protecting national security" the system adopted provides adequate and sufficient guarantees against arbitrariness and the risk of abuse, even if there may be individual aspects of any system which might be capable of being altered or improved. Such an approach properly reflects the role of the Convention, which is to set down "minimum standards" that can be applied across all Member States. Provided that – following an overall assessment – the Court finds that a system for bulk interception provides adequate and sufficient guarantees against arbitrariness and abuse, in view of the very different regimes in operation in different States, it will not be appropriate for it to be too prescriptive about the way in which those regimes should operate (although it may, as it did both in *Centrum För Rättvisa* and in this case, identify those aspects of the regime which could be improved upon). Applying this approach to the Court's supervisory jurisdiction in the present case (as it was in *Centrum För Rättvisa*), the Court should have given due weight to the fact that the domestic courts and authorities have subjected both the UK system as a whole as well as the individual complaints at issue to detailed and extensive scrutiny by express reference to the Convention standards and this Court's case law and should have found that there was, here, no breach of Article 8 of the Convention.

Post Scriptum

26. Since the adoption of this judgment on 3 July 2018, the IPT has handed down yet another judgment in relation to another, unrelated, aspect of the UK's surveillance regime: *Privacy International v Secretary of State for Foreign and Commonwealth Affairs (Rev 1)* [2018] UKIPTrib IPT_15_110_CH (23 July 2018). For obvious reasons this judgment was not available for consideration by the Court when it reached its conclusions on the question of exhaustion of domestic remedies (and we have heard no submissions on it). That said, it seems to us that this careful and detailed judgment provides yet further support (if any was necessary) that, in principle, the IPT is an effective remedy for the purposes of Article 35 § 1

of the Convention which applicants will be required to have exhausted before this Court has jurisdiction to entertain their application.

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix EE

Application No. 24960/15

IN THE EUROPEAN COURT OF HUMAN RIGHTS

BETWEEN:

10 HUMAN RIGHTS ORGANISATIONS

Applicants

-and-

THE UNITED KINGDOM

Respondent

FURTHER OBSERVATIONS OF THE GOVERNMENT OF THE UNITED KINGDOM

I Introduction

1. By way of a letter dated 11 October 2016, enclosing the Applicants' further observations and claims for just satisfaction, the Court invited the Government's response to the claims for just satisfaction and any other observations the Government wish to make.

2. These further observations are submitted in response to that invitation by the Court. They also contain the Government's response to the Third Party interventions that have made in this case[1].

3. The Government has already submitted detailed Observations on Admissibility and the Merits addressing the Intelligence Sharing and s.8(4) regimes (referred to hereinafter as "the Observations"), and responding to the specific questions posed by the Court. The Government adopts, but does not repeat, those Observations and has sought to confine these further Observations to new points of substance which have

[1] Three such interventions have been made by Third Parties: (1) The European Network of National Human Rights Institutions ("ENNHRI"); (2) The Electronic Privacy Information Center and (3) Article 19.

been raised by the Applicants or the Intervenors. Where the substance of the interventions is already addressed in the Government's Observations, the Government cross-refers to the relevant paragraphs of the Observations, rather than repeating their substance. The Government uses the same terminology in this Response as is used in the glossary to its Observations.

I. RESPONSE TO 10 HUMAN RIGHTS FURTHER OBSERVATIONS

4. In common with the way in which the Applicant's have structured their further observations, the Government proposes to address the factual assertions which are now made about the two regimes (Part 1), before making a number of legal submissions in response to the Applicants' further observations (Part 2).

THE FACTS

The section 8(4) Regime – general observations

5. Although the Applicants have correctly moved away from characterising the s.8(4) regime as one of "mass surveillance", they nevertheless seek to portray it as a regime in which the totality of communications across entire networks are the subject of substantive and meaningful invasions of privacy in an arbitrary and disproportionate manner[2].

6. But that is to mis-characterise and over-simplify the process and ignores the surgical precision with which GCHQ does (and is legally obliged to) interrogate bulk data pursuant to its statutory powers.

7. Whilst the Security and Intelligence Agencies (SIAs) do intercept the entire contents of a bearer or bearers under the s.8(4) Regime, they only examine a tiny proportion of communications or communications data from those contents, having chosen to examine them, on the basis of statutory tests of purpose, and requirements of necessity and proportionality. This is focused intelligence gathering. Without this

[2] See, in particular §35-37 and 42-46 of the Applicants' further observations.

capability, much vital intelligence would not be available to the UK for legitimate public protection purposes.

8. As explained in detail in the Observations, the s.8(4) Regime operates in this way as a matter of practical necessity. For technical reasons, it is necessary to intercept the entire contents of a bearer, in order to extract even a single specific communication for examination from the bearer: Observations, §§1.31-1.34.

9. Such an act of interception is characterised by the Court as involving an interference with Article 8(1) ECHR. But in truth, it cannot involve a substantial invasion of individuals' privacy rights unless that communication is selected for examination: in other words, unless a human examines it, or may potentially examine it. The analysis of Article 8 rights must focus upon the stage at which a communication is selected for examination; not simply upon the act of interception in itself. If the analysis fails to do this, it will fail to grapple with the true nature of the s.8(4) Regime, how it works, and what activities it permits. And the position is no different, just because communications passing over a bearer may be held temporarily (often for fractions of a second) while they are electronically filtered and subjected to search terms, to determine whether they are selected for such examination.

10. Thus, what ultimately matters for privacy rights is not the mere fact that data are subject to bulk interception. What matters is the adequacy of the safeguards that either allow or prevent such data from being examined. The Government has set out in detail in its Observations the reasons why those safeguards are well sufficient to secure individuals' Article 8 rights, by reason of the statutory framework in RIPA, the Code, the internal safeguards of the Intelligence Services, the application of tests of necessity and proportionality, and the oversight of the IPT, ISC and Commissioner.

11. A regime that operates on the basis of strict controls governing the selection of data for examination, which limits the statutory purposes for which those data can be selected for examination, and which applies tests of necessity and proportionality to such selection, cannot contravene Article 8 ECHR, merely because at the initial stage

a large amount of data is intercepted. Otherwise, the Court's judgment in *Weber and Saravia v Germany* (app. 54934/00) ("*Weber*"), which established the legal requirements governing the interception of communications in this field, would have been wrongly decided.

12. In short, it is illegitimate to suggest that bulk interception itself inevitably entails a breach of Article 8 ECHR.

The Bulk Powers Review

13. The Independent Terrorism Legislation Reviewer has produced further important factual evidence about the Intelligence Services' bulk interception practices pursuant to the s.8(4) Regime, and the intelligence need for such bulk interception. See the Report of the Bulk Powers Review (David Anderson QC), August 2016 ("the Bulk Powers Review").

14. The Bulk Powers Review evaluated the operational case for various intelligence gathering powers, in the context of the Investigatory Powers Bill (which received Royal Assent on 29 November 2016 as the Investigatory Powers Act, though most of the Act is not yet in force), which is intended to provide a new statutory framework for such powers. One of the powers considered in the Review was bulk interception, i.e. interception currently conducted under the s.8(4) Regime.

15. The Bulk Powers Review provides a helpful summary of the way in which bulk interception under the s.8(4) Regime works at §§2.13-2.18, which emphasises the important distinction between the initial interception and filtering of communications, and their selection for potential examination, set out above:

"2.14 Bulk interception involves three stages, which may be called ***collection, filtering*** *and* ***selection for examination****.*

First stage: collection
2.15 GCHQ selects which bearers to access based on an assessment of the likely intelligence value of the communications they are carrying. GCHQ does not have the capacity, or legal authority, to access every bearer in the world. Instead it focuses its resources on those links that it assesses will be the most valuable. At any given time, GCHQ has access to only a tiny fraction of all the bearers in the world.

Second stage: filtering
2.16 GCHQ's processing systems operate on the bearers which it has chosen to access. A degree of filtering is then applied to the traffic on these bearers, designed to select communications of potential intelligence value. As a result of this filtering stage, the processing systems automatically discard a significant proportion of the communications on the targeted bearers.

Third stage: selection for examination
2.17 The remaining communications are then subjected to the application of queries, both simple and complex, to draw out communications of intelligence value. Examples of a simple query are searches against a "strong selector" such as a telephone number or email address. Complex queries combine a number of criteria, which may include weaker selectors but which in combination aim to reduce the odds of a false positive. Communications that do not match the chosen criteria are automatically discarded. The retained communications are available to analysts for possible examination.

2.18 The application of these queries may still leave too many items for analysts to examine, so GCHQ must then carry out a triage process to determine which will be of most use. The triage process means that the vast majority of all the items collected are never looked at by analysts…"

16. At §§2.19, the Review summarises the two major processes that GCHQ applies to bulk interception (i.e. the "strong selector" process and "complex query" process), observing that (i) the "strong selector" process is in effect a "targeted" process, not a "bulk" process at all, because the selectors used relate to individual targets; and (ii) the "complex query" process permits methods of analysis and selection not available with the "strong selector" process, but in no way permits staff to search through communications *"at will"*. It is *"closer to true bulk interception, since it involves the collection of unselected content and/or secondary data"*. But "*as with the [strong selector process], it remains the case that communications unlikely to be of intelligence value are discarded as soon as that becomes apparent"*.

17. At §2.20, David Anderson QC observes that he has "no reason to disagree" with the ISC's assessment that the s.8(4) Regime does not collect communications indiscriminately, and that *"only the communications of suspected criminals or national security targets are deliberately selected for examination"*.

18. Chapter 5 of the Bulk Powers Review assesses the utility of bulk interception, as carried out by GCHQ under the s.8(4) Regime. That assessment was undertaken on the basis of an intensive review of closed evidence: see §5.2:

"Cathryn McGahey QC and I have inspected a great deal of closed material concerning the value of bulk interception, including warrant renewal applications (which contain details of the use to which intelligence derived from bulk interception had been put) and explanations produced for the benefit of the ISC and the Review."

19. Points made in Chapter 5 include the following:

(1) Just under half of all GCHQ intelligence reporting is based on data obtained under bulk interception warrants. For counter-terrorism intelligence reporting, this figure rises to over half: §5.9.

(2) Targeted interception cannot be viewed as a generally viable substitute for bulk interception. Even where a "strong selector" is known (e.g. a telephone number or email address), it may in an overseas context very often be necessary to intercept in bulk in order to obtain information from that selector. A targeted warrant would very often not produce the same result. See §§5.24-5.33:

(i) The location of some targets may mean that targeted interception would not be practicable (e.g. the target in Syria).

(ii) Even in more favourable overseas locations, the cooperation of local CSPs in giving effect to a targeted warrant might not be forthcoming, or might be possible only after delays.

(iii) The fragmentary nature of global communications, involving the division of communications into packets, means that a targeted warrant would not, or would not necessarily, capture all the information that GCHQ needs.

(iv) The number of overseas targets could render such a regime prohibitively cumbersome.

(v) "Contact chaining"[3] on the basis of targeted interception is a valuable technique, but has limitations. It is dependent upon the Intelligence Agencies already knowing their initial subject of interest; new subjects of interest being in contact with the initial subject; and it being possible to serve a targeted interception warrant on new subjects. Those conditions will not always be satisfied, particularly where subjects of interest are overseas. Moreover, "contact chaining" may very well not work where

[3] That is, identifying terrorist connections through interrogation of data obtained through targeted means, in order to find additional contacts who use the same form of communication.

extremists use a variety of different communications methods in an effort to conceal their activities: §§5.28-5.33.

(3) Bulk acquisition of communications data may in some circumstances be an adequate alternative to bulk interception: but it would not be noticeably less intrusive and would have a disadvantage in terms of speed (and the need for cooperation from CSPs): §5.34.

(4) Similarly, human sources of intelligence may be unavailable, and the obvious dangers to human sources must be taken into account: §5.35.

(5) Thus, in sum, no alternative source of intelligence, or combination of alternatives, would be sufficient to substitute for a bulk interception power: §5.41.

20. In the conclusion to Chapter 5 of the Bulk Powers Review, David Anderson QC revisited the conclusion he reached in the Anderson Report concerning the utility of bulk interception (see Observations, §1.35), and stated:

"5.53 This Review has given me the opportunity to revisit my earlier conclusion with the help of Review team members skilled respectively in technology, in complex investigations and in the interrogation of intelligence personnel, and on the basis of considerably more evidence: notably, a variety of well-evidenced case studies, internal documentation and the statistic that almost half of GCHQ's intelligence reporting is based on data obtained under bulk interception warrants.

5.54 My opinion can be summarised as follows:

(a) the bulk interception power has proven itself to be of vital utility across the range of GCHQ's operational areas, including counter-terrorism in the UK and abroad, cyber-defence, child sexual exploitation, organised crime and the support of military operations.

(b) The power has been of value in target discovery but also in target development, the triaging of leads and as a basis for disruptive action. It has played an important part, for example, in the prevention of bomb attacks, the rescue of a hostage and the thwarting of numerous cyber-attacks.

(c) While the principal value of the power lies in the collection of secondary data, the collection and analysis of content have also been of very great utility, particularly in assessing the intentions and plans of targets, sometimes in crucial situations.

(d) The various suggested alternatives, alone or in combination, may be useful in individual cases but fall short of matching the results that can be achieved using the bulk interception capability. They may also be slower, more expensive, more intrusive or riskier to life."

21. Annex 8 to the Bulk Powers Review contains 13 "case studies", illustrating the use of and need for bulk interception, and providing context and a factual underpinning for the conclusions in chapter 5. 4 of those case studies were summarised (albeit in slightly less detail) in the Anderson Report, as to which see Observations, §1.36. The other nine are summarised below. As with the examples in the Anderson Report, their importance speaks for itself:

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

(2) Following terrorist attacks in France, GCHQ provided support to MI5 and European partners in identifying targets and prioritising leads. GCHQ triaged around 1,600 international leads (in the form of telephone numbers, email addresses or other identifiers) in the days following the attacks. It was necessary quickly to determine whether there was any further attack planning, and to identify leads that should be prioritised for further investigation. Without bulk data, that triage work would have taken much longer – potentially many months – and would have led to GCHQ obtaining an incomplete picture, providing only limited assurance that further attack planning had been identified or ruled out: Case Study A8/3.

(3) During the UK's Afghanistan campaign, analysis of data obtained through bulk interception enabled GCHQ to locate and monitor an armed group that had taken hostages captive. Within 72 hours of the kidnapping, the hostages were located. Analysis of the content of communications obtained through bulk interception indicated that the hostages' lives were in danger. The hostages were successfully rescued. There was no likely alternative method to bulk interception

through which the hostage-takers could have been identified and located, or their intentions revealed: Case Study A8/6.

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

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

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

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

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

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

Response to Applicants' factual allegations about the s.8(4) regime: §§26-32, 35-47

22. At §§26-30 of the Applicants' Further Observations, the Applicants have sought to define the terms "bulk" and "targeted", such that anything which is "bulk" is effectively indiscriminate and is to be contrasted with a "targeted" capability which is based on "*reasonable suspicion that a specific target*" has committed or is likely to commit a criminal offence or is a threat to national security. But that distinction is unhelpful and unjustified in the present context:

    a. To the extent that it implies that, as part of bulk interception, GCHQ in fact accesses communications about a wide range of people who are of no legitimate interest to the security and intelligence agencies, that is wrong. As made clear by David Anderson QC in the Bulk Powers Review, the s.8(4) regime does not permit interference with communications indiscriminately and only the communications of suspected criminals or national security targets are deliberately selected for examination.

    b. This over-simplistic distinction ignores the incremental collection, filtering and selection process which in fact takes place as set out at §§15-16 above. That careful process incorporates significant safeguards at each stage and

ensures that these activities are necessary and proportionate. Thus, whilst there may be "bulk" collection at the first stage, there is then a sequence of stages applied which ensures that the fragments of intelligence which are actually analysed and pieced together at the end of the process are appropriately targeted at those who in fact pose a threat to the UK i.e. individuals who are of legitimate intelligence interest, regardless of whether they had previously been identified as a threat by the SIAs.

c. Allied to that, it is wrong to suggest that selection other than by reference to a previously identified individual must mean that the interception is untargeted and indiscriminate. Even when there is selection at the third stage on the "complex query" basis i.e. by inputting a number of criteria to narrow down the information which is analysed, that does not mean that communications are available for GCHQ analysts to search through at will. As explained in the Bulk Powers Review, the filtering and complex search process draws out the communications of intelligence value and therefore the odds of a 'false positive' are considerably reduced (see §2.21 of that report at p25). Whilst "complex query" process is closer to true bulk interception (since it involves the collection of unselected content and/or secondary data) it would be wrong to categorise that as indiscriminate since that activity must still satisfy the statutory tests of purpose, together with necessity and proportionality, in order to be lawful. As stated by the Commissioner at §6.5.40 of his 2013 Report[4]:

"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."

d. In addition, to the extent that it is suggested that activity can only be lawful for Art. 8 ECHR purposes in this context if it is based on "reasonable grounds for suspicion" that is not consistent with the established case law in this area, as discussed in more detail at §§90-97 below.

[4] See Annex 1

23. In terms of the different stages of the bulk interception process, the three stages outlined in the Bulk Powers Review (see §15 above) set this out authoritatively and accurately and are to be preferred, in contrast to the suggested six stages at §31 of the Applicants' further observations. For example, "Initial interception" and "Extraction" are, in fact, one single process i.e. the information is initially obtained by copying it. Stage 4 is a necessary part of any analysis at Stage 3 and therefore both stages are more accurately described under the rubric of "selection for examination" (see §2.17 of the Bulk Powers Review). In addition Stage 6, i.e. any distribution of the results of analysis to other persons or agencies, is outside the scope of the current application and is subject to separate safeguards and controls.

24. Whilst it is right that s.8(4) sets no upper limit on the number of communications that may be intercepted, it does not follow that, even in principle, a single warrant could "*encompass the communications of an entire city in the UK with the residents of another country*" (see Applicants' further observations at §§35-37). That could never be necessary or proportionate (applying the safeguards set out at §§2.69-2.81 of the Observations). It is also fanciful to suggest that this could occur in practice since this could only possibly occur if all such communications were carried on a single telecommunications system and, in practice, there is extraordinary diversity in the supply of communications technologies to consumers.

25. GCHQ does not seek to contend that the limitations on its resources constitute a permissible legal safeguard in this context (contrary to the suggestion at §§38-40 of the Applicants' further observations). As made clear by the ISC it is <u>both</u> for legal reasons and due to resource constraints that GCHQ cannot conduct blanket indiscriminate interception of all communications and most importantly "*it would be unlawful for them to do so, since it would not be necessary and proportionate, as required by RIPA* (see §58 of the ISC Report set out at §1.23 of the Observations).

26. There is also no inconsistency in the Government's description of GCHQ's operations (see §41 of the Applicants' further observations). Whilst it is right that electronic communications do not traverse the internet by routes which can

necessarily be predicted, that does not mean that the first stage of the process (i.e. collection) is or could lawfully be, indiscriminate or wholly untargeted. For example, there may be a very real difference (in terms of necessity and proportionality) between identifying a bearer which carries a high proportion of e-mail traffic flowing out of Syria from one which carries e.g. You Tube videos between states which are unlikely to be of intelligence interest. Accordingly it is an unfair characterisation of the process to suggest that the first stage of the process involves access to "*an enormous amount of data relating to the lives of private individuals around the world, the vast majority of whom are not and never will be of intelligence interest to UK intelligence services*" (see §41 of the Applicants' further observations). That first stage does involve an element of selection and that is just the beginning of a process which narrows down what is actually analysed to that which is strongly likely to include communications of legitimate interest to the SIAs. The Applicants' submissions effectively boil down to a proposition that it could never be Art. 8 ECHR compliant to intercept in bulk prior to selecting for examination. But that is clearly contrary to this Court's approach in *Weber*.

27. In addition and as discussed above, it is wrong to suggest that GCHQ analysts can store and "*trawl*" through a "*large pool of information...by reference to unknown selectors that may bear little or no resemblance to criminal investigations or operations*" (see Applicants' further observations at §42). Whilst it is not understood what is meant by "unknown selectors" in this context (given that GCHQ cannot be expected to make public the selectors it uses), if this is meant to be a description of the "complex query" process at the selection stage (see §2.21 of the Bulk Powers Review), then the characterisation of that process is wholly inaccurate. These searches are designed to draw out communications of intelligence value and other communications which are not of intelligence interest are discarded. That was the clear conclusion of the ISC and Mr Anderson QC (including in the Bulk Powers Review) i.e. oversight bodies who have direct experience of the process in practice.

28. It follows that the example which is given at §§44-46 of the Applicants' further observations, namely that bulk interception could result in "*everyone's reading activities*" being "*automatically intercepted, stored and made available for analysis*" is

utterly far-fetched. Whilst, in principle, a selector could be used to identify everyone who had downloaded a particular book or article from the internet, there are safeguards in place which ensure that any selector is justified on necessity and proportionality grounds and technical measures are also in place (by way of a triage process) to ensure that a selector which produces too many items for examination is refined before the results can be looked at by an analyst. The sophistication of the selection process ensures that the system is more proportionate, not more intrusive, contrary to the impression given in the Applicants' submissions.

29. It is also misleading to suggest that "*the dragnet of bulk intercept includes routine and automated storage and analysis of the communications of human rights activists*" (§47 of the Applicants' further observations). That could never be necessary or proportionate and was contrary to the express findings of the IPT in its Third Judgment (dated 22 June 2015) in which it made clear that GCHQ had lawfully and proportionately intercepted and selected for examination communications of the two Applicants (as explained in detail at §§4.102-4.103 of the Observations).

Is the Government constrained by NCND in this context? (§§48-52)

30. At §§48-52 of the Applicants' further observations it is said that the Government is not constrained from responding more fully to the factual allegations which have been made about its bulk interception activities and is seeking to hide behind a "self-imposed" policy of Neither Confirm Nor Deny (NCND). It is also suggested that the NCND principle has been called into question by the domestic courts.

31. This ignores the fact that the NCND principle was accepted in *Kennedy v United Kingdom*[5] as a valid basis on which information could be withheld (see §187) and was also recognised in *Klass* at §58, *Weber* at §135 and *Segerstedt-Wiberg v Sweden*, judgment 6 June 2006 at §102. It remains an important mechanism through which the state discharges its positive obligations (including under Arts. 2 and 3 ECHR) to protect information which, if disclosed, would be harmful to the public interest. Most recently in the domestic setting the principle was reviewed by Lord Justice

[5] App. 26839/05, 18 May 2010

Pitchford in the context of the 'Undercover Policing Inquiry'[6] who considered evidence from a Senior Cabinet Office National Security Adviser. There was no suggestion in that careful review of the application of the principle that it was unimportant or capriciously applied (see, in particular, §§116, 127, 145-146 of that Ruling).

'New' facts: §§53-55

32. In terms of the 'new facts' referred to at §§53-55 of the Applicants' further observations (and addressed at §§4-9 of the Applicants' Factual Appendix) these are neither confirmed nor denied. As discussed above, it has been a principle of successive UK Governments neither to confirm nor deny ("NCND") assertions, allegations or speculations in relation to the Intelligence Services, whose work requires secrecy if it is to be effective.

33. In any event, as appears to be acknowledged by the Applicants at §55 of their further observations, these allegations are irrelevant to the issues which have been raised in these applications.

Intrusiveness of interception content and communications data: §§56

34. As explained at §§4.29-4.31 of the Observations, the Court has correctly recognised in *Malone v UK* (app. 8691/79, Series A no.82) that it is less intrusive in Article 8 terms to obtain communications data than the content of those communications. That remains the same even in relation to internet-based communications. The aggregation of 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. However, it remains the case that, if like is compared with like, the interception of communications raises greater privacy concerns. For example, the content of 50 communications is very likely to be more intrusive in

[6]Annex 2. Restriction Orders: Legal Principles and Approach Ruling 3 May 2016:

Article 8 terms than the communications data associated with those 50 communications.

The Intelligence Sharing Regime: §§33-34, 62-77, 226-231

35. In their further observations the Applicants make wide-ranging submissions about the nature of US surveillance law. It is unnecessary and inappropriate for the Court to make findings about that law in this Application.

36. The Applicants' further observations also address alleged US surveillance activities outside the scope of this Application. The Application is about the UK's alleged receipt of information from the USA's Prism and Upstream programmes[7], which the NSA operates under the authority of s.702 FISA. The Applicants address the NSA's surveillance activities under a completely different authority (Executive Order, "EO" 12333) (see §§64-68 and §77 of the Applicants' further observations and see §§10-12 of the Applicants' Factual Appendix). It is unnecessary and inappropriate to address EO 12333.

37. In those circumstances, the Government makes the following key points in response to these aspects of the Applicants' further observations.

38. **First** insofar as the intelligence activities and operations of the US Government have been the subject of official statements and/or other express avowal by the executive branch of the US Government, the Government does not adopt the NCND principle in relation to them. But some caution should be exercised when considering allegations which have not been publicly avowed by the US Government. In that regard the Government wishes to draw to the Court's attention the Executive Summary of the Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden, published by the U.S. House of Representatives on 15 September 2016[8]. In this document the House Permanent

[7] See e.g. Applicants' Additional Submissions on the Facts and Complaints at §§5-8.

[8] Annex 3. Executive Summary of the Review of the Unauthorised Disclosures of Edward Snowden published on 15th September 2016

Select Committee on Intelligence finds that "*the public narrative popularized by Snowden and is allies is rife with falsehoods, exaggerations, and crucial omissions*" (p1). They also find that it is "*not clear Snowden understood the numerous privacy protections that govern the activities of the [U.S. Intelligence Community]. He failed basic annual training for NSA employees on Section 702 of the Foreign Intelligence Surveillance Act (FISA) and complained the training was rigged to be overly difficult. This training included explanations of the privacy protections related to the PRISM program that Snowden would later disclose*" (p3). The Committee concluded that Snowden "*was, and remains, a serial exaggerator and fabricator. A close review of Snowden's official employment records and submissions reveals a pattern of intentional lying*" (p3).

39. **Secondly** it is incorrect to suggest that Presidential Policy Directive 28 ('PPD-28') places no restrictions on the collection of signals intelligence in bulk (see §64 of the Applicants' further observations). PPD-28 requires that "[*s]ignals intelligence activities shall be as tailored as feasible*" and, as noted in the Letter from Robert Litt, General Counsel of the Office of the Director of National Intelligence dated 22 February 2016 ('the Litt Letter')[9] "*[t]his means, among other things, that, whenever practicable, signals intelligence collection activities are conducted in a targeted manner rather than in bulk*".

40. **Thirdly** it is wrong to characterise Upstream and Prism as "bulk" programmes, in direct contrast to programmes which are "targeted" (see §71 of the Applicants' further observations and §§13-19 of their Factual Appendix). As made clear by David Anderson QC in the Bulk Powers Review, although the powers under FISA s.702 do concern "bulk interception" the powers are focused and targeted and bear a strong resemblance to GCHQ's 'strong selector' process. That was made clear at §§3.56-3.65 of that Report, including in the following passages:

"***There are marked similarities between the s702 programme and bulk interception as practised in the UK, particularly via the "strong selector process"*** *summarised at 2.19(a) above:*

(a) Both are ***foreign-focused capabilities****, based on the interception of a cable and the collection of "wanted" communications* ***by the application of strong selectors.***

[9] at 4-6 (Annex VI to the Privacy Shield documents) (http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf).

(b) The application of those selectors from a very early stage ***gives both the flavour of targeted capabilities****, though as explained at 2.19(a) above, the holding of communications in bulk for a short period means that a bulk warrant will be required under the Bill.*

(c) Both offer the advantages of operational scale and flexibility to service the range of foreign intelligence missions.

(d) Even the authorisation regimes are similar, with external authorisation of the intelligence purposes for which the data can be accessed and used and the procedures for targeting and handling of information, but with decisions relating to individual selectors being delegated to GCHQ / NSA.

...

The s702 arrangements continue to permit the ***targeted selection*** *and retention by the NSA of wanted communications from bulk internet traffic, in very much the same way as the strong selector process described at 2.19(a) above.* (emphasis added)

41. In those circumstances, the Applicants are wrong to assert that David Anderson QC "endorsed" Upstream as a non-targeted capability in the Bulk Powers Review.

42. Collection under s.702 of FISA is based on specific and identified targets and it may not be carried out on an indiscriminate basis. It must comply with the Fourth Amendment to the US Constitution, statutory restrictions contained in s.702 itself, and Court-approved targeting procedures.

43. The activities under s. 702 must be targeted at specific selectors such as e-mail addresses or phone numbers. The Privacy and Civil Liberties Oversight Board (PCLOB) found that the US government must make targeting "*determinations (regarding location, U.S. person status, and foreign intelligence value) about the users of each selector on an individualized basis[;] it cannot simply assert that it is targeting a particular [ ] group*."[10] The PCLOB's report led to the European Commission's finding, in its adequacy decision assessing the EU-U.S. Privacy Shield Agreement, that acquisition pursuant to s. 702 is "*carried out in a targeted manner through the use of individual selectors that identify specific communications facilities, like the target's e-mail address or telephone number, but not key words or even the names of targeted individuals*."[11]

[10] PCLOB Report at 21.
[11] *See* Adequacy Decision at para. 81 (p. 22), *available at* http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf.

44. Collection activities under s. 702 are also limited to specific and defined intelligence priorities set by policy-makers.[12] These priorities include topics such as nuclear proliferation, counterterrorism, and counter-espionage.

45. "Upstream collection" involves the acquisition of communications as they transit the telecommunications "backbone" networks (including the Internet "backbone") of US telecommunications-service providers.[13] Tasked selectors are sent to providers operating these networks after the government applies its targeting procedures to each individual selector.[14] Upon receipt of the tasked selectors, the service providers must assist the Government in acquiring communications to, from, or otherwise containing these selectors while they transit the 'backbone.'[15] Communications are filtered for the purpose of eliminating wholly domestic communications, and then scanned to capture communications containing tasked selectors.[16] Communications that successfully pass both these filtering screens are then ingested into NSA databases.[17]

46. Before communications facilities may be targeted for intelligence collection, a written certification must be submitted to and approved by the FISA Court[18] which must include targeting procedures.[19] The targeting procedures ensure that collection takes place only as authorised by statute and within the scope of the certifications. Under these limitations, as the PCLOB concluded, collection "*consists entirely of targeting specific persons about whom an individualized determination has been made*."[20]

47. Collection is targeted through the use of individual selectors, such as email addresses or telephone numbers. To target these selectors, US intelligence personnel must

[12] *See* Letter from Robert Litt, General Counsel of the Office of the Director of National Intelligence, dated Feb. 22, 2016, at 4-6 (Annex VI to the Privacy Shield documents) (http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf) (Litt Letter), discussed below.
[13] *See* PCLOB Report at 35; PRG Report at 141 n.137.
[14] See PCLOB Report at 36.
[15] PCLOB Report at 35–37. *See also* Litt Letter.
[16] PCLOB Report at 37.
[17] *Ibid*.
[18] 50 U.S.C. §1881a (a) and (b) – the FISA Court is a US federal court established and authorized under the Foreign Intelligence Surveillance Act of 1978 (FISA).
[19] *See* 50 U.S.C. § 1881a (d).
[20] *See* PCLOB Report at 103.

determine, pursuant to targeting procedures approved by the FISA Court, that they are likely being used to communicate foreign intelligence information that falls within the categories covered by the certification submitted to the court.[21] The reasons for selecting a target must be documented[22].

48. The Department of Justice and ODNI (Office of the Director of National Intelligence) review the documentation for every selector to assess compliance with the requirements of the targeting procedures – i.e. that all three requirements are met: that the user is reasonably believed to be (i) a non-US person, (ii) located outside the US, and (iii) who there is a valid foreign intelligence reason for targeting.[23]

49. As part of its review of the certification, the FISA Court must assess the targeting and minimization procedures against the reasonableness requirements of the Fourth Amendment. While the targeting and minimization procedures are primarily concerned with the privacy of US persons, the targeting procedures require that before a non-US person's selector is targeted for s.702 acquisition, the US government must include a written explanation for each individual tasking decision. This tasking decision contains the basis for the government's determination that collection on the particular target will likely return foreign intelligence information relevant to the subject of one of the certifications approved by the FISA Court.[24]

50. Thus, the targeting procedures protect the privacy of non-US persons by ensuring that each individual targeting decision is based upon a sufficient nexus to the foreign intelligence information sought to be obtained by one of the FISC-approved certifications. Similarly, the written certification approved by the FISA Court must include minimization procedures. The minimization procedures for s.702 have been

[21] 50 U.S.C. §1801(e). For example, the US might target the user of a specific email address or telephone number based on credible information indicating that the email address or telephone number (a "selector") is believed to be used by a foreign terrorist operating overseas.
[22] For example, the government would specify how it was able to reasonably assess that the selector is used by a foreigner located outside the US and what foreign intelligence information (e.g., terrorism) the government expects to obtain from targeting the user of the selector.
[23] 50 U.S.C. §1881a(l); *see also* NSA Director of Civil Liberties and Privacy Report, *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702* (hereinafter "NSA Report") at 4, available at http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.
[24] *See* PCLOB Recommendations Assessment Report, February 5, 2016, at 14-15.

publicly released.[25] These procedures focus on US persons but also provide important protections to non-US persons.

51. The US Intelligence Community must also comply with the privacy protections afforded to non-US persons by Presidential Policy Directive 28 (PPD-28) – see §§1.13-1.14 of the Observations (and see also the Litt Letter). This extends certain protections afforded to the personal information of US persons to non-US person information (and see further §141 below)[26].

52. In those circumstances, the programmes which are carried out under the authority of s.702 of FISA can properly be described as "targeted" and certainly do not involve the indiscriminate bulk collection of data.

53. **Finally**, in §69 of their further observations, the Applicants refer to media reports which describe Prism (collection under s.702 of FISA) as a programme under which the US was "*tapping directly into central servers*". However, as the Applicants concede in the Factual Appendix (see §19), that statement is inaccurate. An accurate description of how the programme operates can be found in the PCLOB Report dated July 2014 (see the Observations at §1.8).

LEGAL FRAMEWORK

The Applicants' summary of the legal framework §§82-126

54. The Government has set out in detail the legal framework which applies to the Intelligence Sharing and s.8(4) regimes at pp59-103 of the Observations. In terms of the Applicants' further observations on the current legal framework, the Government makes the following key submissions in response.

[25] The minimization procedures are available at http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf; http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf; and http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf.

[26] NSA's unclassified and publicly available PPD-28 procedures apply to all of NSA's signals intelligence activities, including activities undertaken under s.702 - *see, e.g.*, NSA PPD-28 Implementation Procedures, Section 7.2.

55. As regards the intelligence sharing regime:

    a. It is inaccurate to say (at §89 of the Applicants' further submissions), that when the Applicants initiated proceedings in the IPT there was "*no information in the public domain setting out the rules governing intelligence sharing between the UK Government and foreign intelligence agencies*". As set out at §§2.1-2.22 of the Observations that regime was set out in primary legislation.

    b. In terms of the Disclosure which was recorded in the IPT's 5 December and 6 February Judgments (see §93 of the Applicants' further observations), since it formed part of a judicial decision it can be taken into account in assessing "forseeability" for Art. 8(2) ECHR purposes – see the Observations at §2.23 and footnote 63. Therefore, prior to being incorporated into the Code, the domestic position was the same as a result of the 5 December 2014 and 6 February 2015 IPT judgments.

56. In terms of the oversight provided by the Investigatory Powers Tribunal (see §§96-100 of the Applicants' further observations):

    a. The IPT decision in *Human Rights Watch v Secretary of State for the Foreign and Commonwealth Office et al* [2016] UKIP Trib 15/165/CH, 16 May 2016, was a response to a worldwide campaign by Privacy International which encouraged individuals to bring claims in the IPT in order to find out "*if GCHQ illegally spied on you*". When addressing whether a sample of claimants had victim status to bring ECHR claims, the IPT applied the recent guidance in *Zakharov v Russia*, 4 December 2015, Application No. 47143/06[27]. That was

[27] The IPT concluded: "*We are satisfied that the appropriate test for us to operate, which would accord with Zakharov and our obligations under RIPA, is whether in respect of the asserted belief that any conduct falling within subsection s.68(5) of RIPA has been carried out by or on behalf of any of the Intelligence Services, there is any basis for such belief; such that the "individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or legislation permitting 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). This continues to be the low hurdle for a claimant that this Tribunal has traditionally operated*."

not an "abandoning" of the approach noted by this Court in *Kennedy*[28]; it was a legitimate application of the victim test at §171 of *Zakharov*. As the IPT itself noted in the final sentence of §46 of its judgment "*This continues to be the low hurdle for a claimant that this Tribunal has traditionally operated.*"

b. There is nothing improper, as a matter of principle, in the IPT receiving briefings from the SIAs as part of their work. The IPT is a specialist tribunal and the nature of its casework means that it is necessary for its members to have a level of background understanding regarding the agencies' practices and procedures. The meeting which occurred at Thames House on 28 September 2007 (as recorded in a Note for File dated 15 November 2007) was an entirely appropriate example of that and the suggestion that it somehow undermines the independence or effectiveness of the IPT is strongly resisted.

c. As is clear from a proper reading of the Note for File which recorded that meeting:

   i. The purpose of the visit was a "general briefing", including about MI5's data handling techniques and the growth and changes to MI5 and the scale of the threat that it was facing.

   ii. As part of the data handling presentation MI5 indicated that, for the purposes of IPT proceedings, it would not routinely conduct searches of "reference data-bases" i.e. databases containing information about the population generally (e.g. the Voter's Roll or telephone directories), for any mention of a complainant's name and such searches would only be carried out if the data was "*relevant or had been relied on in the course of an investigation*" (see Annex C to the Note for File).

   iii. That was an entirely sensible and proportionate suggestion, since the fact that a complainant's name was on e.g. a Voter roll which had

[28] See the Applicants' further observations at §97.

never been accessed by officers at MI5 could not conceivably be relevant to whether there had been unlawful conduct in relation to an individual.

iv. As made clear from the Note for File the meeting was an opportunity for MI5 to make clear what its standard position would be. It would be open to the IPT on a case by case basis and in response to any particular complaint to decide that such an approach should not be followed and to require more extensive searches as necessary[29].

> Indeed, that has very recently occurred in domestic proceedings in the IPT concerning the lawfulness of bulk personal datasets, where the IPT has ordered the Respondents to carry out searches of their databases (including their Bulk Personal Datasets and Bulk Communications Datasets)"[30]

d. In addition, it cannot sensibly be suggested that this meeting in any way undermines the independence or effectiveness of the IPT's examination of the s.8(4) or intelligence sharing regimes:

i. The complaints were not about the holding of bulk personal datasets i.e. "reference data-bases" which have been the subject of separate and more recent proceedings in the IPT[31]. They were about interception under the s.8(4) RIPA regime and intelligence sharing with the US. (Similarly, in these proceedings, there is no complaint about the use of bulk personal datasets, which are the subject of an entirely different legal regime and therefore wholly outwith the scope of the application.)

[29] That is consistent with the standard form of words which MI5 uses when responding to an IPT complaint which makes clear the position it has adopted as regards searches of reference data. That standard form of words is as follows: *""When checking our records in response to complaints to the IPT, we would not normally search reference databases containing information about the general population, eg the electoral roll, telephone directories etc, for a trace of the complainant's name. We would only do so if it appeared relevant to the complaint and/or the Tribunal specifically requested it. This was discussed and agreed with Tribunal members when they visited Thames House on 28 September 2007. In this case, we have not checked reference databases for any mention of Mr [name redacted]. If the Tribunal requires us to do so, please let us know*."

[30] IPT Bulk Data Directions Searches Order 12 December (Annex 8 attached)

[31] Annex 4. See the recent judgment of the IPT in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs & Others* [2016] UKIPTrib 15_110-CH

ii. The meeting occurred six years before the Applicants brought claims in the IPT and only one of those who attended the meeting was part of the panel of five who heard the complaints.

iii. The Applicants' suggestion that reference data such as the Voter's roll or telephone directories should have been searched as part of their complaint about "bulk interception" is therefore not understood.

iv. The searches which were conducted in the IPT proceedings were plainly adequate, not least because unlawful conduct was identified in respect of two of the complainants.

v. The IPT was assisted throughout the proceedings by Counsel to the Tribunal (CTT) who was able to make submissions (as appropriate) on the adequacy of the search process by GCHQ and the other respondents (GCHQ being the primary respondent given the nature of the allegations in the proceedings).

57. In addition, the Applicants' criticisms of the ISC and the Commissioner are misplaced (see §§101-107 of the Applicants' further observations). Whatever the position historically, it cannot be said that the ISC has devoted little attention to scrutinising the Government's interception programmes, as is evident from its detailed report in March 2015 discussed at e.g. §§1.3, 1.19, 1.21, 1.23-1.24, 1.26, 1.33 of the Observations.

58. As to the suggestion that the part-time status of the Commissioner means that he is unable to provide effective oversight, that has not been suggested by the Commissioner himself. In his 2013 Annual Report he stated that his investigations are "*thorough and penetrating*" and that he has "*no hesitation in challenging the public*

authorities wherever this has been necessary" (at §6.3.3[32]). That sentiment was also reiterated e.g. in his 2015 Annual Report[33].

59. At §§108-115 and §137 of the Applicants' further observations it is said that certain proposed changes to the UK domestic legal framework for investigatory powers, as set out in the Investigatory Powers Bill 2016 (which received Royal Assent on 29 November 2016 as the Investigatory Powers Act, though most of the Act is not yet in force), demonstrate that the current legal framework is "unfit for purpose" and that the Government's position in these proceedings is "unsustainable". But it is important to recognise that the Investigatory Powers Act deals with a wide range of powers, the vast majority of which are beyond the scope of this application. The intention of the Act is to provide an up to date framework for the use (by the SIAs, law enforcement and other public authorities) of investigatory powers to obtain communications and communications data[34]. It addresses not just the interception of communications, but also the retention and acquisition of communications data and equipment interference activity. It will essentially consolidate and build upon the range of current statutory powers in these areas.

60. That a need has been identified for the updating and consolidating of existing legislation, cannot lead to the conclusion that the s.8(4) regime or the intelligence sharing regime is unlawful. That was not the conclusion of the IPT, having investigated these matters in considerable detail. Nor was that any part of the Joint Committee's Report on the Draft Investigatory Powers Bill (see §113 of the Applicants' submissions), whose remit was not to opine on the compatibility of those two regimes with the ECHR[35].

[32] Annex 1. ***Commissioner's Annual Report 2013***

[33] Annex 5. Commissioner's Annual Report 2015. At 2.2 he stated: "*The Commissioner is independent of Government and Parliament and must report half-yearly7 to the Prime Minister on the carrying out of his functions. Independent oversight plays a key role in contributing to accountability. The purpose of oversight is to ensure that there are strong checks and balances, demanding and visible safeguards, and that public authorities are held to account*."

[34] See the Explanatory Notes to the Bill at Annex 7.

[35] See the Joint Committee on the Draft Investigatory Powers Bill, Report, HL Paper 93-HC 651 at Annex No. 26 of the Applicants' Reply. The role of the Joint Committee was to conduct pre-legislative scrutiny of the draft Bill and to make recommendations about the Bill.

Applicants' summary of the procedural history: §§116-126

61. The Government has set out the procedural history to these Applications at pp53-59 of the Observations. In particular it is to be noted that the Applicants are wrong to suggest that they were not represented at the closed hearing on 10 September 2014 at which time the IPT considered the sensitive arrangements governing the s.8(4) and intelligence sharing regimes. As explained at §§7.32-7.35 of the Observations Counsel to the Tribunal (CTT) was appointed in the domestic IPT proceedings and, in practice in this case, performed an essentially similar function to that of a special advocate (see §10 of the 5 December judgment). In those circumstances it is misleading to state that there was no one representing the interests of the applicants in the closed hearing.

LEGAL SUBMISSIONS

Intercepting communications data is as intrusive as intercepting content: §§-134

62. The general answer to this assertion is set out at §§4.29-4.33 and 4.57-4.64 of the Observations i.e. in summary:

    (1) The Court has correctly recognised in *Malone v UK* (app. 8691/79, Series A no.82) that it is less intrusive in Article 8 terms to obtain communications data than the content of those communications (see §34 above).

    (2) As a result, the Court has rightly not applied the *Weber* safeguards to the acquisition of communications data (as opposed to content).

    (3) Similarly, the Court has not applied the *Weber* safeguards to other forms of surveillance (e.g. the installation of GPS in a suspect's car – see *Uzun v Germany* app. 35623/05): which is a strong indicator that the *Weber* criteria should not apply to the acquisition of related communications data under the s.8(4) Regime.

    (4) Therefore, the test should be the general one whether the law indicates the scope and manner of any discretion with sufficient clarity to give the individual

adequate protection against arbitrary interference. The s.8(4) Regime satisfies that test as regards communications data, for all the reasons in §§4.57-4.64 of the Observations.

(5) In any event, it should be noted that the s.8(4) Regime distinguishes between communications content, and "related communications data". "Related communications data" has a specific statutory meaning which is not synonymous with "metadata", or "behavioural data. Much "metadata" or "behavioural data" is content for the purposes of the s.8(4) Regime, and is thus subject to the controls for content. For example, information about the internet pages that a user visits on a particular site would be content, not RCD for the purposes of the s.8(4) Regime.

(6) Further, if the *Weber* safeguards did apply to "related communications data", those safeguards would on a proper analysis be met by the s.8(4) Regime.

63. As explained at §§4.17-4.27 of the Observations, *Digital Rights Ireland* is not relevant to the current application, not least because that case did not concern a national regime or any provision governing access to, or use of, retained data by national law enforcement authorities. Nor does the quotation from §27 of the judgment (see §130 of the Applicants' further observations) address the comparative level or intrusiveness as between content and communications data.

64. Further the Advocate General in *Tele2 Sverige* & *Watson*[36] was addressing (in Part 6 of his opinion) the proportionality of "*general data retention obligations*" (§250) including "*the retention of data relating to all communications effected within the national territory procure in the fight against serious crime*" (§251). It was in that specific context that he referred to the risks associated with access to such data being great or even greater than those arising from access to the content of communications (§§257-259). And he specifically contrasted "*targeted surveillance measures*" when reaching these conclusions which he considered were different from "*general data retention obligations*" (§256). For the avoidance of doubt, the Government reserves the right to

[36] Joined Cases C-203/15

make further submissions on the relevance of these proceedings once judgment has been handed down by the CJEU.

65. Similarly it is not correct to equate any powers to obtain related communications data under the s.8(4) regime with the US's telephony collection programme under s.215 of the USA Patriot Act ("the s.215 Power") (see §§133 of the Applicants' further observations).

    a. First it is to be noted that PCLOB found not only that the s.215 Power raised serious constitutional concerns, but also that it had *"shown minimal value in safeguarding the nation from terrorism"*. In part as a result of PCLOB's findings, the s.215 Power was allowed to lapse by the USA, and was replaced by a different programme under the USA Freedom Act which addressed the issues raised by PCLOB.

    b. Secondly, the collection of telephony metadata pursuant to the s.215 Power is not remotely equivalent to powers exercised pursuant to the s.8(4) Regime. The s.215 Power did not concern interception at all. It authorised the bulk acquisition of telephone records generated by certain telephone companies in the United States, and their storage in a single database. That is not what the s.8(4) Regime authorises, or does. Rather, the closer analogue to the s.8(4) Regime is the USA's surveillance programme under s.702 FISA: a power that PCLOB found to be both constitutional and of high and increasing value. See generally the Bulk Powers Review at §§3.50-3.65 and §§40-52 above.

Forseeability and accessibility: §§135-138

66. To the extent that it is sought to be suggested that *Zakharov* introduces any new (and heightened) test of forseeability in this context, that is not accepted. In this context, the essential test remains 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*. The Grand

Chamber confirmed in *Zakharov* that this test remains the guiding principle when determining the foreseeability of intelligence-gathering powers (see §230).

Internal versus external communications: §§139-

67. This has been addressed in detail at §§4.66-4.76 of the Observations. In addition:

a. It was very well understood at the time RIPA was passed that the s.8(4) Regime would necessarily entail the interception of all communications flowing down a bearer or bearers; and that this would mean intercepting both "internal" and "external" communications. Precisely those points were made in Parliament by Lord Bassam of Brighton when the Bill which became RIPA was debated: see Observations, §1.37. Moreover, RIPA itself provides for, and authorises, the necessary interception of internal communications in the course of the execution of a s.8(4) warrant for the interception of external communications: see s.5(6) RIPA.

b. The description in Mr Farr's witness statement of how the definition of "external communications" in s.20 RIPA applies to particular forms of internet-based communication is no more than the application of a clear definition to certain common and current forms of internet usage. In any event, and as already explained in the Observations, the question precisely how the definition of "external communication" applies to particular forms of internet usage is substantially irrelevant to the operation of the s.8(4) Regime. See Observations, §§4.71-4.76.

c. Contrary to what is asserted at §§141-142 of the Applicants' further observations, the distinction which Mr Farr draws between communications which are received inside and outside the UK is entirely consistent with what was said to Parliament (and what is set out in the Code). If e.g. a communication is received by a platform in the US and is intended to be seen by a wide audience then it is logical that it would be classified as 'external' (see Mr Farr at §§134-138). Moreover, Mr Farr also makes the point (see §137

of his statement) that if e.g. an e-mail is being sent to a specific individual, then the question whether or not the communication was internal or external would depend upon where that individual was located and not on how the e-mail was routed. Consequently there is nothing in Mr Farr's evidence which contradicts the assurances given to Parliament when RIPA was debated.

d. The Government has accepted that the nature of electronic communications over the internet means (and has always meant) that the *factual* analysis of whether a particular communication is internal or external may, in individual cases, be a difficult one (see §4.70 of the Observations). But any such difficulties in how the distinction applies to any *particular* communication is irrelevant in circumstances where it is in practice inevitable (and entirely foreseeable) that, when intercepting material at the level of communications links, both internal and external communications will be intercepted (see §4.71 of the Observations).

e. Importantly the safeguards at the selection for examination stage for communications intercepted under a s.8(4) warrant do not make any distinction between internal or external communications: the safeguards apply equally to both. That means that the s.16 safeguards are not somehow "lost" for UK-based persons if their communications are categorised as external communications (see §§4.73-4.76 of the Observations)[37].

f. Any complexities which may arise in practice in terms of the definition of external and internal communications, do not demonstrate an "apparent indifference" towards the importance of ensuring that there is a clear and accessible regime for bulk interception (as asserted at §§146-147 of the Applicants' further observations). It is a recognition that the way in which

[37] For example, in the case of a Google search, or a YouTube viewing, if the searcher or viewer were in the British Islands, GCHQ could only have selectors that were referable to them as they would be the only individual in relation to whom communications with Google and YouTube could be selected, and such selection would accordingly be done in accordance with the requirements of s.16 RIPA. Whether the communication to be selected were in fact external or internal would be irrelevant. Their interception under the applicable s.8(4) warrant would be lawful (whether by virtue of s.8(4) or s.5(6)(a)), but GCHQ could not examine them if the Secretary of State had not certified that their examination was necessary by means of a modification to the certificate accompanying the s.8(4) warrant (see §4.75 of the Observations).

modern communications systems work will, in practice, inevitably lead to difficult decisions as to how particular communications can be categorised under any legal system. It also involves a proper focus on the essential test for forseeability, namely 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* and §230 of *Zakharov*. The safeguards which apply regardless of whether the communication is internal or external are central to that.

The framework for analysing the claims: §§148-156

68. The Applicants assert that there is a material difference between the strategic monitoring considered in *Weber* and the s.8(4) regime (see §§148-150). They also assert that the "minimum safeguards" in *Weber* are no longer sufficient to address modern forms of communication surveillance (§§152-156 of the Applicants' further observations).

69. Neither proposition is correct. First there are close parallels with the regime which was considered in *Weber,* as explained in detail at §§4.11-4.12 of the Observations. To assert, as the Applicants do, that the persons liable to be affected by s.8(4) are "*every person who uses the internet*" is a gross and inaccurate exaggeration for the reasons explained in detail at §§5-29 above. It is also important to recognise that the test is not whether, in one or more respects, the s. 8(4) Regime is somehow broader or less tightly defined than the German strategic monitoring regime at issue in *Weber*, not least because the strategic monitoring in that case 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.

70. Secondly to the extent that it is suggested that the decision of the Fourth Section in *Szabo* suggests that the minimum safeguards in *Weber* need to be enhanced in this particular context, that is not accepted.

71. The observations made in *Szabo* were made in the context of a regime which, it was found, allowed ordering of interception entirely by the Executive, with no assessment of strict necessity, with potential interception of individuals outside the operational range and in the absence of any effective remedial or judicial measures (see §17 and §52). Those cumulative factors led the Court to find a violation of Article 8 ECHR. Crucially (and pertinent to the distinction between mass interception and mass surveillance) the Court found there to be no or no adequate controls preventing the examination of communications following interception.

72. In the judgment the Court expressly acknowledged that bulk interception was proportionate in order to meet modern security threats, but that the issue was whether the applicable safeguards were adequate, at §68:

> "[I]*t is a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies in pre-empting such attacks, including the massive monitoring of communications susceptible to containing indications of impending incidents* […] *In the face of this progress the Court must scrutinise the question as to whether the development of surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights*".

73. Insofar as the Court identified a need to enhance Convention case-law on interception (§70), this was for the purpose of addressing surveillance practices, specifically involving the acquisition and retention of detailed profiles of intimate aspects of citizens' lives. As addressed in detail at the outset of these further Observations (and at §§1.21-1.25 of the main Observations), the s.8(4) regime is not one of "mass surveillance".

Alleged absence of mandatory minimum safeguards: §§157-183

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

74. At §§159-160 of the Applicants' further observations it is suggested that bulk interception cannot be lawful in the absence of suspicion that a particular offence has been or may have been committed.

75. This is not what the law requires. It is not mandated by Article 8 ECHR, and it would in practice denude the interception of communications under the s.8(4) Regime of a very large portion of its utility, thereby endangering the lives of UK citizens.

76. Much of the aim of interception pursuant to the s.8(4) Regime is not to search for the communications of identified targets. Rather, it is to ascertain, via the application of complex searches, who should be a target in the first place ("target discovery"). It is to identify who are the individuals, groups and organisations outside the UK that pose a threat to the UK, because without such a power the Intelligence Services would be unable to tell who they were. See for example the Bulk Powers Review at §5.3:

"Bulk interception is a capability designed to obtain foreign-focused intelligence and identify individuals, groups and organisations overseas that pose a threat to the UK. It allows the security and intelligence agencies to intercept the communications of individuals outside the UK and then filter and analyse that material in order to identify communications of intelligence value.

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

(Emphasis added)

77. See too Annex 7 to the Bulk Powers Review, which sets out GCHQ's "Statement of Utility of Bulk Capabilities", supplied to the Review in July 2016, stating inter alia:

"GCHQ would not be able to identify those who wish us harm without bulk powers. Terrorists, child abusers, drug traffickers, weapons smugglers and other serious criminals choose to hide in the darkest places on the internet. GCHQ uses its bulk powers to access the internet at scale so as then to dissect it with surgical precision.
By drawing out fragments of intelligence from each of the bulk powers and fitting them together like a jigsaw, GCHQ is able to find new threats to the UK and our way of life; to track those who seek to do us harm, and to help disrupt them.

- ***Bulk Interception:*** *Interception provides valuable information that allows us to discover new threats. It also provides unique intelligence about the plans and intentions of current targets – through interception of the content of their communications. Communications data obtained through bulk interception is also*

> *crucial to GCHQ's ability to protect the UK against cyber-attack from our most savvy adversaries and to track them down in the vast morass of the internet."*

(Emphasis added)

78. See also the ISC's Report[38] at vii on page 3 ("Key Findings"), under the heading "Why do the Agencies intercept communications?"

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

79. Turning to the various examples of the use of bulk interception powers under the s.8(4) Regime given in Appendix 8 to the Bulk Powers Review, and set out at §22 above, well over half of the examples concern the discovery of previously unknown targets through the use of a bulk interception capability, instead of (or in addition to) the tracking of known targets. The need to undertake target discovery in the present circumstances is readily apparent from the increased terrorist threat in Europe, as exemplified by the state of emergency in France following the Paris attacks of November 2015.

80. Further, even where a known target has been identified, the reasonable basis for targeting that individual's communications may not be that they are themselves engaged in planning or committing criminal acts. A person may be a legitimate intelligence target whether or not they are involved in criminality or analogous acts: for instance, an employee of a hostile foreign government, or a person in contact with a terrorist.

81. In this context, the requirements of s.5 of RIPA, as read with the relevant definitions in s.81 of RIPA and with §§6.11-6.12 of the Code are plainly sufficient as recently affirmed by this Court in *RE v United Kingdom* at §133.

(2) The categories of people liable to have their communications intercepted: **§§161-169**

[38] Annex 6 to the Observations.

82. For the reasons set out at §5-29 above it is not correct that the initial interception stage is indiscriminate or "virtually limitless" as sought to be contended for by the Applicants (and whether in terms of communications data or otherwise). Consequently the material differences with the regime in *Weber* are not accepted. As set out at §4.42 of the Observations, the categories of persons liable to have their communications intercepted are sufficiently identified at the interception stage.

83. As regards §167 of the Applicants' further observations:

    a. The certificate sets out the categories of communications that GCHQ may examine and the categories directly relate to the intelligence-gathering priorities set out by the Joint Intelligence Committee and agreed by the National Security Council (see ISC Report at §100, 3rd bullet and see also the Code at §6.14).

    b. The Commissioner confirmed in his 2013 Report that the certificate is regularly reviewed and is subject to modification by the Secretary of State (see §6.5.43 and also see the evidence of Mr Farr at §80).

    c. The oversight of the certificate which is provided by the Commissioner is also made clear in the Code (at §6.14) which states: "*The Interception of Communications Commissioner must review any changes to the descriptions of material specified in a certificate.*"

    d. The ISC report also makes clear that the Foreign Secretary was satisfied that "*strategic environmental issues*" reflect a legitimate UK requirement for intelligence (see §103).

    e. As stated at §104 of the ISC Report, following a review by the Foreign Secretary, the certificate is reviewed at least annually by the Secretary of State.

In those circumstances there are substantive limitations on the categories of people whose information can be selected for examination.

(3) Limits on the duration of interception: §170

84. It is not accepted that the time limits in s.9(6) of RIPA are "effectively meaningless". There can be no "long-term rolling renewals" of warrants since there are safeguards in place to ensure that any renewals are necessary and proportionate:

    a. 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[39]). 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."

    b. 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.

    c. §6.27 of the Code also 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).

(4) The procedure to be followed for examining, using and storing the data obtained: §§171-178

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

85. The Government's detailed case on this topic is to be found at §§4.51-4.53 of the Observations. In terms of the further criticisms which have been made by the Applicants, the Government responds by making the following key points:

    a. 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:

        i. 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.

        ii. 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*".

    b. The programmes referred to at §172 of the Applicants' further observations are neither confirmed nor denied and in any event do not form the subject matter of this application.

    c. Whilst it is right that internal communications can be read if they are selected by reference to a factor which is not by reference to an individual known to be in the British Islands, there are extensive safeguards in place to protect against arbitrary interference. Those are set out at §4.52 of the Observations and have been largely ignored by the Applicants. In addition the system ensures that, even if it is subsequently discovered that an individual is

actually in the UK, when previously that was not known, the SIAs must cease all action at that point (see §112(iv) of the ISC Report).

d. As to the suggestion that s.16(3) of RIPA does not provide the same rigour as a s.8(1) warrant, this is not accepted, as explained at §4.44 of the Observations. In addition, David Anderson QC, after investigating the position in detail in his report 'A Question of Trust', concluded as follows at §6.56(a):

"Most UK-based individuals who are subjects of interest to the security and intelligence agencies or law enforcement are however targets of s8(1) warrants issued by the relevant Secretary of State, which will authorise the interception of all their communications, where necessary with the assistance of GCHQ."

e. It is not the case that there is no regulation or oversight of the use of selectors and search criteria:

i. The detail of the s.15 and s.16 RIPA arrangements is kept under review by the Commissioner (see §4.53 of the Observations).

ii. The Code contains express provisions which require records to be kept of the arrangements for securing that only material which has been certified for examination (in accordance with the statutory purposes and tests of necessity and proportionality) is, in fact, read, looked at or listened to (see §6.28 and §§7.16-7.18 in the context of s.16 RIPA). In practice that means that a necessity and proportionality justification must be prepared for any selectors and search criteria which are used.

f. Finally the IPT's Third Judgment dated 22 June 2015 does not support the contention that the procedures for examining, using and storing data are inadequate. That single error does not undermine the overall effectiveness of the safeguards. In addition it is to be noted that the IPT concluded that the "*the selection for examination was proportionate*" (see §15). The Tribunal also indicated that it was "*satisfied that no use whatever was made by the intercepting*

agency of any intercepted material, nor any record retained, and that the Sixth Claimant has not suffered material detriment, damage or prejudice as a result of the breach."

(5) The precautions to be taken when communicating intercepted material to other parties: §§179-181

86. The Applicant's suggestion that there should be a requirement for individualised reasonable suspicion is addressed in detail at §90-97 below.

87. As to the safeguards for the dissemination of intercepted information and any related communications data, it is to be noted that s.15(2) of RIPA is supplemented by the Code and by the constraints imposed by other primary legislation as explained at §4.52(4) and §2.92 of the Observations.

(1) In addition the Applicants have misread *Weber* in the submissions made at §180. At §40 of Weber it was noted that the Federal Constitutional Court had made clear that the transmission of data was proportionate if it served an important legal interest and if there was a sufficient factual basis for the suspicion that "*criminal offences were being planned or had been committed*" (emphasis added). Given that any disclosure under the s.8(4) regime must satisfy the requirements of s.15(2) as supplemented by 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, there is not a material difference between the s.8(4) regime and the strategic monitoring system in *Weber* in this regard.

(6) The circumstances in which data obtained may or must be erased or the records destroyed: §§182-183

88. The Applicants' case that these safeguards are "unclear" is not understood. For the reasons set out at §4.54 of the Observations this requirement is obviously met.

89. There is also no suggestion in the IPT's Third Judgment of 22 June 2015 that the "technical"[40] retention period error in respect of Amnesty International was a systemic problem. Had that been the case the IPT can be expected to have said so in that judgment. In addition the IPT specifically addressed this in its judgment in *Human Rights Watch v Secretary of State for the Foreign and Commonwealth Office et al* [2016] UKIP Trib 15/165/CH, 16 May 2016, at §44, concluding that:

> *"We are satisfied that there was not... some kind of systemic or wide-ranging failure by the Respondents by virtue of what was disclosed in Liberty/Privacy No 3. There were, as described in paragraphs 5 and 6 above, two relatively minor breaches of procedure."*

Further minimum safeguards? §§184-200

No requirement for individual reasonable suspicion

90. At §§185-187 of their further observations the Applicants assert that there should be a minimum requirement of reasonable suspicion that a sender or recipient has committed an offence. In support of that contention the Applicants rely on *Zakharov* and *Szabo*.

91. The true principle to be derived from the authorities on Article 8 is that any interception of and access to communications must be necessary and proportionate, and must satisfy the *Weber* criteria, which the s.8(4) Regime does: see Observations, §§4.40-4.56. Any attempt to frame a narrower rule which (for example) outlaws any interception, save where a target has already been identified before the interception takes place, is contrary to the whole thrust of the Court's case law, which permits "strategic monitoring": see *Weber,* where the challenge to the German state's regime in this respect was not only dismissed, but declared manifestly ill-founded. The Applicants impermissibly elevate the Court's particular findings on the specific facts

[40] See §14 of the IPT's Third Judgment dated 22 June 2015 where the IPT stated: "*We are satisfied however that the product was not accessed after the expiry of the relevant retention time limit, and the breach can thus be characterised as technical, though (as recognised by the Tribunal in the Belhadj Judgment) requiring a determination to be made. Though technical, the breach constitutes both "conduct" about which complaint may properly be made under section 65 of RIPA and a breach of Article 8 ECHR… The Tribunal is satisfied that Amnesty… has not suffered material detriment, damage or prejudice as a result of the breach, and that the foregoing Open Determination constitutes just satisfaction, so there will be no award of compensation."*

of certain cases into statements of general principle, rather than findings on particular facts in a particular context.

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

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

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

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

(1) It is the totality of safeguards against abuse within the system that is to be considered. See e.g. *Zakharov* at §§257, 270-271.

(2) Where a decision has been made to target a particular individual, it will be necessary for a judicial authority to be able to review that decision on its merits (i.e. to determine not simply whether it was taken in accordance with proper procedures, but to assess whether it was necessary and proportionate). See *Zakharov*.

(3) However, such judicial oversight can be either *ex ante* or *post facto*: see e.g. *Szabo* at §77, *Kennedy* at §167.

(4) The s.8(4) Regime provides such oversight. It is able to, and will, examine the necessity and proportionality of any interception or examination of the complainant's communications, with the benefit of full access to the evidence. See Observations, §§2.39-2.45.

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

97. For the reasons explained at §§13-21 above, the Bulk Powers Review demonstrates that the bulk interception powers in the s.8(4) regime are necessary and proportionate, even where the intelligence services are searching for the communications of individuals who have not already been identified as a target and in order to identify threats to the UK. That does not "obviate" any meaningful

assessment of proportionality as that Review and the case studies referred to therein amply demonstrate.

Prior independent authorisation: §§188-193

98. The suggestion that there should be prior independent authorisation of s.8(4) warrants has been comprehensively addressed at §§4.96-4.99 of the Observations. That this is not a minimum requirement was made expressly clear in *Szabo* at §77. This is a situation in which there is extensive independent (including judicial) *post factum* oversight.

99. Neither *Digital Rights Ireland* or *Tele 2 & Watson* (Advocate General Opinion) are relevant in this context. Neither of those cases lay down definitive mandatory requirements relevant to the present context and the Government reserves the right to make further submissions on the latter case following the judgment from the CJEU.

Subsequent notification of interception measures: §§194-200

100. As to the suggestion that there should be a minimum requirement of subsequent notification to individuals of interception measures:

a. That was not a proposition which was advanced domestically before the IPT in these proceedings.

b. As set out above, the *Szabo* decision has to be read in the context of a regime which was entirely deficient in terms of safeguards of the Executive action in question. The Court reached its determination on the basis that there was a failure to comply with the *Weber* minimum safeguards and it was unnecessary for the Court to embark on the question whether enhanced guarantees were necessary (§70). Accordingly, there was no suggestion that the Court was laying down further minimum requirements over and above the *Weber* minimum criteria and there was no indication in §86 that

subsequent notification of surveillance measures was such a requirement. As the Court noted at §86 it was the *combination* of a complete absence of safeguards plus a lack of notification which meant that the regime could not comply with Art. 8 ECHR.

c. The Opinion of the Advocate General in *Tele 2* & *Watson* does not support the proposition that there should be a minimum requirement of notification. §236 of his Opinion (cited at §195 of the Applicants'' further observations) was addressing the question of supervision by an independent body, not subsequent notification of data retention (or surveillance measures).

d. Finally it is not correct to say that the Commissioner has been "strongly critical" of "unnecessary limitations" on his oversight (see §§199-200 of the Applicants' further observations). The matters set out at §200 of the Applicants' further submissions formed part of a "wish list" of elements which the Commissioner would have like to have seen in the Investigatory Powers Bill 2016 to strengthen the current oversight of surveillance powers. It was not a suggestion that the current s.8(4) regime was unlawful without subsequent notification to individuals of surveillance measures.

Necessity and proportionality of the s.8(4) regime: §201-214

101. At §§201-214 of the Applicants' further observations it is said that the "bulk interception regime" is unnecessary and disproportionate. In this regard the Government repeats §§4.84-4.95 of the Observations and makes the following additional points.

Strict necessity

102. 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.

103. To the extent that the Applicants rely on *Szabo* for the proposition that a test of "strict necessity" is required, 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 Convention 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.

104. 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.

The necessity and proportionality of the s.8(4) regime

105. The rationale for the s.8(4) Regime and its operation have been addressed on a number of occasions by independent bodies, viz. the IPT, the ISC, the Commissioner, the Anderson Report, and the Bulk Powers Review. Materially, the Anderson Report, the Bulk Powers Review and the ISC in its report of 17 March 2015 (the ISC Report) all conclude in terms, and with supporting analysis and detail, that less intrusive (or different) programmes could not address legitimate needs of the UK. See above and Observations, §§1.21-1.35.

106. Although it is correct that the Independent Reviewer in the Bulk Powers Report was not specifically tasked with opinion on whether bulk interception powers were proportionate (see §204 of the Applicants' further observations), the conclusions of that review and plainly highly material to that question, as summarised at §§13-21 above. At §§9.12-9.14 he stated:

"I have already summarised what I consider to be the strength of the operational case for each of the bulk powers (chapters 5-8 above). Among the other sources of evidence referred to in chapter 4 above, I have based my conclusions on the analysis of some 60 case studies, as well as on internal documents in which the SIAs offered frank and unvarnished assessments of the utility and limitations of the powers under review.

The sheer vivid range of the case studies – ranging from the identification of dangerous terrorists to the protection of children from sexual abuse, the defence of companies from cyber-attack and hostage rescues in Afghanistan – demonstrates the remarkable variety of SIA activity. ***Having observed practical demonstrations, questioned a large number of analysts and checked what they said against contemporaneous intelligence reports, neither I nor others on the Review team was left in any doubt as to the important part played by the existing bulk powers in identifying, understanding and averting threats of a national security and/or serious criminal nature, whether in Great Britain, Northern Ireland or further afield.***

My specific conclusions, in short summary, are as follows:

(a) ***The bulk interception power is of vital utility across the range of GCHQ's operational areas, including counter-terrorism, cyber-defence, child sexual exploitation, organised crime and the support of military operations. The Review team was satisfied that it has played an important part in the prevention of bomb attacks, the rescuing of hostages and the thwarting of numerous cyber-attacks. Both the major processes described at 2.19 above [i.e. the "strong selector" and "complex query" process] produce valuable results. Communications data is used more frequently, but the collection and analysis of content has produced extremely high-value intelligence, sometimes in crucial situations. Just under 50% of GCHQ's intelligence reporting is based on data obtained under bulk interception warrants, rising to over 50% in the field of counter-terrorism."*** (emphasis added)

107. In the light of the conclusions of this review, to describe the Government's bulk interception as "*a speculative fishing exercise, designed to check the behaviour of an entire population*" (see §212 of the Applicants' further observations) could not be further from the truth. It is a capability which is of "*vital utility*" in identifying, understanding and averting threats of a national security and/or serious criminal nature.

108. As to the Applicants' reliance on cases involving the bulk *retention* of data (see §§203, 207-209 of the Applicants' further observations), those are irrelevant to the issues raised in this application which involves bulk interception followed by

targeted selection of material. This is not a situation where there is bulk retention of data on an "indiscriminate" basis (see §§207-208 of the Applicants' further observations).

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

The lawfulness of the intelligence sharing regime: §§232-250

110. At §§232-250 of the Applicants' further observations it is submitted that "*the standards applicable to interception*" under Art 8 ECHR should also apply "*when access is given to intercepted material even if the actual initial interception was carried out by a foreign intelligence service*"[41].

111. The assertion that the *Weber* safeguards should apply to the sharing of intelligence between the US and UK is misguided, for reasons set out in the Observations at §§3.29-3.36. In short summary:

a. There is no Article 8 case of the Court suggesting that the *Weber* criteria should be applied in the distinct factual context where the intelligence agencies of the respondent State have merely obtained information from a foreign State.

b. The Court has expressly indicated that the "rather strict standards" developed in recent Strasbourg intercept cases do not necessarily apply in other intelligence-gathering contexts[42].

[41] See, in particular, §243.
[42] See Observations at §3.32.

c. There is no good reason to single out intercepted communications/communications data from other types of information that might in principle be obtained from a foreign intelligence agency, such as intelligence from covert human sources or from surveillance. In many cases, the Intelligence Services may not even know whether information from an intelligence agency does derive from interception. Moreover, there is no particular reason why such information should be more sensitive than information from any other source. But it would not plainly be neither feasible nor (from a national security perspective) safe for a domestic legal regime to set out all the various types of intelligence that might be obtained from a foreign State; define the tests to be applied when determining whether to obtain them, and the limits on access; and set out the handling, etc. requirement and the uses to which all such types of information might be put.

112. This is not to place form over substance (see §§235-236 of the Applicants' further observations). 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.

113. There is also no contradiction in the Government's policies, including in the Code. Whilst the Government has been able to formulate rules for the requesting and handling of 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) (see §239-240 of the Applicants' further observations), that does not mean that it would be feasible to formulate rules for all the different types of information which might be shared by foreign governments. 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 any 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).

114. As to the suggestion that the intelligence sharing regime was substantively defective prior to December 2015 (as well as being insufficiently signposted in public) (see §§246-247 of the Applicants' further observations), for the reasons set out at §§90-99 above, there is no requirement for prior judicial authorisation or any requirement for individual reasonable suspicion.

115. In terms of the Disclosure which was recorded in the IPT's 5 December and 6 February Judgments (see §248 of the Applicants' further observations), since it formed part of a judicial decision it can be taken into account in assessing "forseeability" for Art. 8(2) ECHR purposes – see the Observations at §2.23 and footnote 63. Therefore, prior to being incorporated into the Code, the domestic position was the same as a result of the 5 December and 6 February judgments.

116. It is also inaccurate to speak merely of a "note" setting out the Government's policy. The substance of the note was reflected in the IPT's judgments and is now set out in the Code, which is itself "law" for the purposes of the "in accordance with the law" requirement (see e.g. *Kennedy* and §3.38 of the Observations). In any event the Disclosure is also "law" for these purposes: it is a published statement, contained in publicly accessible court judgments.

117. Finally there is no merit in the criticism that the Disclosure (as now reflected in Chapter 12 of the Code) is obscurely drafted or vague (see §248(2)-(4) of the Applicants' further observations).

a. It is clear that the terms "request" and "receipt" would cover all the scenarios where the SIA that carry out the relevant activities can access material intercepted by foreign intelligence agencies in the circumstances mentioned in §248(2). The access to databases or raw material referred to at §248(2) of the Applicants' further submissions would, on a straightforward application of the Code, be covered by it.

b. The concepts of "analysed" and "unanalysed" are also sufficiently clear (§248(3)). They are ordinary English words, which require no further definition. Material which has been automatically scanned and selected, but which has not been examined, is "unanalysed"; and material which has been examined, and conclusions drawn about it in the form of a report or analysis, is "analysed".

c. It is wrong to suggest that there is no protection for communications data (§248(4)). As set out at §12.6 of the Code where communications content or communications data (and whether or not the data is associated with the content of communications) are obtained by the intercepting agencies or otherwise received from a government of another state in circumstances where the material identifies itself as the product of an interception, it must be subject to the same internal rules and safeguards that apply to the same categories of content or data when they are obtained directly by the intercepting agencies as a result of interception under RIPA.

Victim Status

118. The Government does not repeat the submissions about victim status made at §§3.2-3.6 and §4.1 of the Observations. For the avoidance of doubt the Government made clear in its Observations that it was accepted that the South African Legal Resources Centre and Amnesty International did satisfy the victim test in the context of the s.8(4) regime – see §4.1 of the Observations and see §255 of the Applicants' further observations.

119. As regards the intelligence sharing regime, the US programmes referred to at §256 of the Applicants' further submissions, which are said to operate under Executive Order 12333, do not form the subject-matter of this application, which is specifically limited to the Prism and Upstream programmes (which are authorised under s.702 of FISA). In those circumstances it is impermissible for the Applicants to seek to rely on those programmes in support of the contention that they are victims for the purposes of the intelligence sharing regime complaints.

Article 14 ECHR: §§262-271

120. This is addressed in detail at §§8.1-8.16 of the Observations.

121. In terms of whether there is a relevant difference of treatment:

a. It is not the case that the IPT came to the conclusion that the s.16 safeguards have a "disproportionately prejudicial effect" on non-British nationals (see §266 of the Applicants' further observations). That was the *submission* which was made to the IPT by the Applicants, as recorded at §144 of the First Judgment (5 December 2014). But the IPT did not have to determine that submission, because it reached the very clear conclusion that any difference in treatment could, in any event, be justified (see §148 of the First Judgment and the reference to "*any indirect discrimination is sufficiently justified*"). In those circumstances the Government is not seeking to challenge a finding which was made by the IPT in this regard (as suggested at §§265-266 of the Applicants' further observations).

b. As regards the Applicants' analysis of *Magee v United Kingdom*[43], including with reference to *Carson v United Kingdom* App. No. 42184/05, 16 March 2010, any difference in treatment is not on the grounds of "residence" (see §70 of *Carson*), but on the grounds of current location. That is not a relevant difference of treatment for the purposes of Art. 14 ECHR.

[43] App. No. 28135/95, ECtHR 6 June 2000

122. On the question of justification (even if there is (which is denied) a relevant different of treatment), the Applicants' further observations (§§270-271) can be answered as follows:

a. The field of national security is a paradigm example of where a state's margin of appreciation is wide – see *Weber* at §106, *Klass* at §49, *Leander* at §59, *Malone* at §81. The *Stec* test is not inappropriate in the present context (see §271(3) of the Applicants' further observations);

b. The factors relied upon by the Government in support of any difference in treatment were compelling and obvious and are not in any way diminished by a lack of witness evidence to support them. It was "*quite plain*" to the IPT that "*the imposition of a requirement for a s.16(3) certificate in every case would radically undermine the efficacy of the s.8(4) regime, given the pre-eminent role of that regime in the identification of threats to UK national security from abroad*" (§148 of the First (5 December 2014) judgment). There is no proper basis for this court departing from that conclusion of the expert domestic tribunal in this area.

c. There is no inconsistency between the Government's case and its explanation of how the s.8(4) regime works. As set out at §16 above, the selection stage of the s.8(4) process may involve "strong selectors" but it can also involve the "complex query" process. In many cases the SIAs will not know who the individual is and that is wholly unsurprising given the current nature of the terrorist threat which the UK faces – as discussed at §§8.14-8.16 of the Observations.

d. Finally the distinction is not irrational for the reasons explained at §§8.13-8.16 of the Observations. The Government has a panoply of powers to investigate a person present in the UK and that distinction justifies any relevant difference in treatment.

Article 6 ECHR

Determination of civil rights and obligations

123. The suggested distinctions which are asserted by the Applicants at §§272-277 of the Applicants' further observations are unsustainable. In determining whether Art. 6(1) applies to the Applicants' complaints it cannot be relevant whether a domestic tribunal already exists or not. The question is whether the supervisory measures in question are within the scope of the definition of 'civil rights' in Art. 6(1). As recognised by the Grand Chamber in *Ferrazzini* at §24[44], that concept is "autonomous" 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.

124. In *Klass* the Commission reached the clear conclusion that Art. 6 does not apply to state interference on security grounds and there is no good reason why that should not apply in this context. That approach is entirely consistent with the Court's more general jurisprudence on the meaning of "civil rights and obligations" for the reasons set out at §§7.6-7.8 of the Observations.

Fairness

125. The Applicants have raised two new matters which they say are relevant to the assessment of whether the IPT proceedings were compliant with Art. 6(1) ECHR (assuming it applied). They rely on the 28 September 2007 meeting at Thames House (see §§281-283 and also §§98-100 of the Applicants' further observations) and they

[44] App. No. 44759/98, 12 July 2001

also rely on the administrative error which the IPT initially made in its Third Judgment when it mistakenly attributed a finding on breach of Art 8 ECHR to the wrong complainant.

126. In terms of the meeting of September 2007 (recorded in a Note for File dated 15 November 2007) this has been addressed at §§56(b)-(d) above. There is no merit in the suggestion that this undermines the independence or effectiveness of the IPT nor can there be any sensible suggestion that the searches which were conducted in this case were not reasonable or proportionate.

127. As to the reliance on the error made by the IPT, the IPT made clear in its letter dated 1 July 2015 that there had been a mistaken attribution in the judgment which arose after all judicial consideration had taken place and 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.

Article 10 ECHR

128. The Article 10 ECHR aspect of the complaints has been addressed in detail at §§6.2-6.39 of the Observations. In response to the Applicants' further observations at §§286-294, the Government makes the following key points:

a. It is to be noted that it was agreed between the parties during the IPT proceedings that, save for the question of prior judicial authorisation, no separate argument arose in relation to Article 10(2), over and above that arising under Article 8(2) (see the IPT's First Judgment dated 5 December 2014 at §149).

b. The Applicants rely on *Sanoma Uitgevers BV v The Netherlands*[45] (see §290 of their further observations), but that was a case concerned with targeted measures to compel disclosure of journalistic sources rather than a regime of strategic monitoring in the course of which journalistic (or NGO) material might be intercepted (*Weber*). It was in that context that the Court identified the importance of prior authorisation by a Judge or other independent body.

c. It is not correct to characterise the relevant provisions of the Code (which do not exhaustively define "confidential communications") as "*nothing more than restatements of "considerations" which may be taken into account*" (see §293 of the Applicants' further observations). As set out at §6.26 of the Observations the Code provides for a series of practical steps which must be taken in terms of the retention, destruction, handling and dissemination of confidential information and that includes notifying the Commissioner of any such material which is retained and making any such information available to him on request.

d. As to proportionality and necessity, the Applicants do not explain how it would be practical or feasible to screen out human rights NGO's privileged communications from the collection stage of the s.8(4) interception regime. It is also material to note that the IPT was entirely satisfied that the communications of Amnesty and the South African Legal Resources Centre had been "lawfully and proportionately" intercepted and accessed/selected for examination (see §§14-15 of the Third Judgment dated 22 June 2015). The effect of the Applicants' submissions is that it could never be necessary or proportionate to subject human rights NGO's communications to s.8(4) activity or the intelligence sharing regime and that is contradicted by the specific findings which the IPT made in these cases.

JUST SATISFACTION – PARA 24

[45] [2011] EMLR 4

129. The Government notes that the Applicants' position is that a reasoned finding of breach of the Convention would be sufficient just satisfaction and they do not seek their costs (see §24 of the Applicants' further observations). In those circumstances it is unnecessary for the Government to make any substantive submissions on this topic.

II REPLY TO INTERVENORS' SUBMISSIONS

European Network of National Human Rights Institutions ("ENNHRI")

Article 6 ECHR: §§8-17

130. ENNHRI's submissions on Article 6 ECHR proceed on a fundamental misunderstanding of what occurred in the domestic IPT proceedings. In particular:

a. The IPT did not "refuse" to direct disclosure of the SIA's sensitive internal guidance concerning the treatment of NGO material. As set out in detail at §§7.37-7.38 of the Observations, the IPT reasonably and appropriately concluded that the issue of NGO confidence had been raised far too late in the domestic proceedings to be considered and the IPT cannot properly be criticised for taking that approach.

b. The IPT did not refuse to consider the Respondents' NCND policy. By agreement between the parties that issue did not arise for determination by the Tribunal (see §13 of the First Judgment dated 5 December 2014).

c. It is not correct to state that the Applicants were not represented in the closed hearing – as explained at §§7.43-7.44 of the Observations the Applicants had the benefit of CTT who was instructed to represent their interests during the closed hearing. Overall there was no unfairness in the procedures which were adopted.

d. In addition, CTT was able to make submissions on the sensitive arrangements which were relevant to the complaints.

131. At §§12 of ENNHRI's submissions it is said that the proceedings in the IPT must have involved the determination of "civil rights" because this was a situation whereby a "judicial body was entrusted with a judicial task". This has been addressed at §119 above. 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.

132. For the reasons set out in detail at §§7.11-7.50 of the Observations, even if Art. 6(1) did apply to the IPT proceedings, those proceedings were fair. To the extent that it is suggested at §16 of ENNHRI's submissions that proceedings could never be fair (whether under the ICCPR or the ECHR) in circumstances where a party is not provided with full disclosure, that is in direct conflict with the decision in *Kennedy v United Kingdom*, where 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 (see §§7.26-7.31 of the Observations). The decision in *ZZ (France) v SSHD*[46] (relied upon by ENNHRI at §17) also acknowledges the possibility of derogation from disclosure requirements for reasons of national security: see §§57-59 and §§64-69. It is not authority for the proposition that there could never be circumstances in which sensitive material was considered in the absence of a party to proceedings.

Article 10: §§18-30

133. The relevance of the case law and other sources cited at §§22-26 of ENNHRI's submissions is not understood. This is not a situation where there has been punishment, prosecution/imprisonment or suppression of journalists or NGOs, nor can it sensibly be suggested that this jurisprudence applies "indirectly" (see §28 of ENNHRI's submissions).

[46] Case C-300/11

134. In terms of the definition of "national security" (see §24 & §27 of ENNHRI's submissions), for the reasons set out at §§4.77-4.81 of the Observations that concept is not "amorphous" in the way it applies to the to the s.8(4) regime, which is designed to ensure that a person's communications cannot be examined simply by reference to unparticularised concerns of "national security". Further, the s.8(4) regime does have precisely those checks and balances to prevent misuse which are called for at §29 of ENNHRI's submissions, for the reasons set out at §§4.32-4.83 and §§6.2-6.30 of the Observations and §§62-89 above.

135. The s.8(4) regime is also proportionate (whether under Art 8 or Art 10 ECHR) for the reasons explained at §§4.84-4.95 and at §§101-109 above.

Article 14: §§31-38

136. As to ENNHRI's submissions on Article 14 ECHR:

a. This is not a situation where there is discrimination on the grounds of nationality. Any difference in treatment is on the grounds of current location and that is not a relevant difference of treatment for the purposes of Art. 14 ECHR, as explained at §§8.3-8.5 of the Observations and at §121 above.

b. In addition, even if there is a relevant difference of treatment (which is not admitted) it is clearly justified for the reasons given at §§8.7-8.16 of the Observations and at §122 above. It is to be noted that ENNHRI's submissions do not attempt to engage with the rational justification for any difference of treatment which is relied upon by the Government and which was straightforwardly accepted by the IPT in its First Judgment of 5 December 2014 – see §§141-148 of the First Judgment dated 5 December 2014.

Electronic Privacy Information Centre ("EPIC")

137. The EPIC submissions make wide-ranging and inaccurate submissions about the nature of US surveillance and US Surveillance law. It is unnecessary and

inappropriate for the Court to make findings about that law (or indeed any future developments in it) in this Application.

138. The EPIC submissions also address alleged US surveillance activities outside the scope of this Application. The Application is about the UK's alleged receipt of information from the USA's PRISM and Upstream programmes, which the NSA operates under the authority of s.702 FISA[47]. EPIC's submissions address the NSA's surveillance activities under a completely different authority (Executive Order, "EO" 12333). It is unnecessary and inappropriate to address EO 12333.

139. It is also unnecessary to address any US activities under s.215 of the US Patriot Act. As set out at §65 above and at §1.7 of the Observations, any activities under that power are of no relevance to this application.

140. As to the allegation that the Upstream and Prism programmes (governed by s.702 FISA powers) are "*largely ignored by US oversight bodies*" and lack legal protections for non-US persons (see §§12-13 of EPIC's submissions), that is not accepted. The Government repeats the submissions made at §§40-52 above. In addition:

141. The US Government's authority to collect "foreign intelligence information" under s.702 of FISA is limited by a number of requirements which have to be examined together to appreciate the limits on this activity.

a. **First**, whilst the definition of "foreign intelligence information" in s. 702 includes "*information with respect to a foreign power or foreign territory that relates to . . . the conduct of the foreign affairs of the United States*" (see 50 U.S.C.

[47] See e.g. Application §4: "*The two programmes which are challenged by this Application are:*
4.1 The soliciting or receipt and use by the UK intelligence services ("UKIS") of data obtained from foreign intelligence partners, in particular the US National Security Agency's "PRISM" and "UPSTREAM" programmes (herafter "receipt of foreign intercept data"), and
4.2 The acquisition of worldwide and domestic communications by the Government Communications Headquarters ("GCHQ")…"
(Emphasis added).

§1801(e))[48], the US may only target specific non-US persons located outside of the US who possess or who are likely to communicate foreign intelligence information that is tied to a specific topical certification issued by the US Attorney General and the US Director of National Intelligence and approved by the Foreign Intelligence Surveillance Court (FISC or FISA Court).

b. More specifically, as part of the US government's application to the FISC, the Attorney General and Director of National Intelligence must specify the categories of foreign intelligence information that the US government is seeking to acquire.[49] And before the certification can be approved, the FISC must determine that the identified categories of foreign intelligence information intended to be collected by the certifications meet the statutory definition of foreign intelligence information.[50] FISC opinions also make clear that s. 702 collection is targeted and must be specifically tied to an identifiable certification. [51]

c. **Secondly**, collection activities under s. 702 must be targeted in the manner described at §§40-52 above.

d. The targeting procedures protect the privacy of non-US persons by ensuring that each individual targeting decision is based upon a sufficient nexus to the

[48] Specifically, 50 U.S.C. § 1801(e) provides:

(e) "Foreign intelligence information" means--

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against--

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to--

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

[49] *See* the July 2014 report on s.702 by the Privacy and Civil Liberties Oversight Board (PCLOB), an independent executive branch agency (hereafter the PCLOB Report), at 23.

[50] *See* PCLOB Report at 6.

[51] *See* FISC Opinion by Judge Hogan reauthorizing certification in 2014. https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.

foreign intelligence information sought to be obtained by one of the FISC-approved certifications. Similarly, the written certification approved by the FISA Court must include minimization procedures. The minimization procedures for s.702 have been publicly released.[52] These procedures focus on US persons but also provide important protections to non-US persons.

e. For example, communications acquired under s. 702, whether of US persons or non-US persons, are stored in databases with strict access controls. The data may be reviewed only by intelligence personnel who have been trained about the minimization procedures and who have a reason to access the data.[53] The data can only be queried to identify foreign intelligence information or, in the case of the FBI only, evidence of a crime.[54] The minimization procedures (and PPD-28, discussed below) limit how long data acquired pursuant to s. 702 may be retained.[55] Further, the information may be disseminated only if there is a valid foreign intelligence or law enforcement purpose; the mere fact that one party to the communication is not a US person is insufficient.[56] Moreover, NSA's s. 702 minimization procedures state that non-US person communications may only be retained, used, and disseminated "*in accordance with other applicable law, regulation, and policy*."

[52] The minimization procedures are available at http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf; http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf; and http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf.

[53] *See* NSA Report at 4.

[54] *See, e.g.*, NSA Minimization Procedures at 6-7, *available at* http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf.

[55] *See* NSA Minimization Procedures, *supra* n. 29; PPD-28 Section 4.

[56] FBI PPD-28 procedures available at http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties. *See also* "USSID SP0018: Supplemental Procedures for the Collection, Processing, Retention and Dissemination of Signals Intelligence Information and Data Concerning Personal Information of Non-United States Persons" (January 12, 2015) (NSA PPD-28 Implementation Procedures).

f. **Thirdly**, collection activities under s. 702 are limited to specific and defined intelligence priorities set by policy-makers.[57] These priorities include topics such as nuclear proliferation, counterterrorism, and counter-espionage.

g. **Finally**, collection activities conducted pursuant to s.702 must comply with the privacy protections afforded to non-US persons by Presidential Policy Directive 28 (PPD-28) - see §§1.13-1.14 of the Observations (and see also the Litt Letter). This extends certain protections afforded to the personal information of U.S. persons to non-U.S. person information[58]. It explicitly provides that the personal information of non-U.S. persons acquired during the US' signals intelligence operations shall be afforded privacy protections comparable to the protections afforded to US persons. PPD-28 and IC elements' implementing procedures are publicly available. For example, the NSA Supplemental PPD-28 Procedures state that the United States Signals Intelligence System (USSS) must, "*[w]henever practicable, use one or more selection terms in order to focus collection on specific foreign intelligence targets (e.g., a specific, known international terrorist or terrorist group)*" and the procedures further provide that the USSS "*may not disseminate [personal information of a non-US person] solely because of a person's foreign status*."[59] Additionally, subject to only limited exceptions, NSA is prohibited from retaining information collected pursuant to its signals intelligence activities for more than five years. Section 4(a)(i) of PPD-28.

142. In those circumstances the assertion that US Law does not provide adequate oversight or protection for the collection of non-US persons' data (see §§11-13, §19 and §28-30 of EPIC's submissions) is simply untrue.

Global Campaign for Free Expression (Article 19)

[57] *See* Letter from Robert Litt, General Counsel of the Office of the Director of National Intelligence, dated Feb. 22, 2016, at 4-6 (Annex VI to the Privacy Shield documents) (http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf) (Litt Letter), discussed below.

[58] NSA's unclassified and publicly available PPD-28 procedures apply to all of NSA's signals intelligence activities, including activities undertaken under s.702 - s*ee, e.g.*, NSA PPD-28 Implementation Procedures, Section 7.2.

[59] *See* Sections 4.2 and 7.2 of NSA PPD-28 Implementation Procedures.

143. Article 19's submissions are premised on the erroneous basis that the UK SIA's engage in the "*indiscriminate interception, storage and analysis of online communications*" (see §3). As explained in the Observations and at §§5-21 above, that is an inaccurate description of the s.8(4) regime.

144. As to Article 19's submissions at §§4-6, it is to be noted that the Government has accepted (at 6.1 of the Observations) that 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 ECHR 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".

145. As set out in more detail in the Government's Observations (§§6.2-6.9), the principles to be applied regarding the Applicants' Article 10 challenge are materially the same as those relevant to the Article 8 question. The Government reiterates the Court's finding to this effect in *Telegraaf Media* (§90), where it held that the essential requirements of lawfulness were the same for both articles, and observed that the two apparently different provisions ("*in accordance with the law*" in Article 8 and "*prescribed by law*" in Article 10) were identical in the French text of the Convention (where both require that interference be "*prevue(s) par la loi*", §89).

146. Despite Article 19's detailed submissions to the effect that bulk interception might have a chilling effect on the freedom of NGOs and the press (see §§10-14) the proper and proportionate response to these concerns is not, as Article 19 would appear to suggest, a prohibition on bulk interception. It is to ensure that any interception of journalistic or NGO material, if and when that occurs through the operation of the s.8(4) interception regime, be subject not only to the statutory safeguards enshrined in RIPA which apply to all intercepted data (*inter alia*, the requirement of certification with explicit justification, limitations on duration of

interception and disposal of material), but be subject also to the enhanced safeguards set out in the Code.

147. In terms of the submissions at §§15-24 of Article 19's intervention and the particular reliance placed on the September 2014 report of the UN Special Rapporteur, his call for states to justify "*with particularity*" the tangible counter-terrorism advantages which had accrued from "*mass surveillance technology*" was based on extremely broad assumptions about the type of activity which might be taking place (including in the US), which does not accurately reflect the s.8(4) regime[60].

148. Similarly, the reports relied upon at §§25-27 of Article 19's submissions, which, in large part address indiscriminate, untargeted, secret collection of data under "mass surveillance programmes" bear no relation to the s.8(4) regime, as properly understood. The *Digital Rights Ireland* case is also irrelevant for the reasons set out at §§4.17-4.27 of the Observations.

149. The assertion that surveillance must be targeted and based on reasonable grounds for suspicion (with particular reliance on *Zakharov v Russia*) has been addressed at §§90-97 above and those submissions are not repeated.

150. The suggestion that there should be prior independent authorisation of s.8(4) warrants has been comprehensively addressed at §§4.96-4.99 of the Observations. That this is not a minimum requirement was made expressly clear in *Szabo* at §77. This is a situation in which there is extensive independent (including judicial) *post factum* oversight.

Anna McLeod

[60] For example, his reference to collecting "*all communications all the time indiscriminately*" (at §18, p7) and "*the systemic interference with the Internet privacy rights of a potentially unlimited number of innocent people located in any part of the world*" (at §59, p21) are not a fair or accurate characterisation of the s.8(4) regime.

Anna McLeod

Agent of the Government of the United Kingdom

16 December 2016

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix FF

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 in principle 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 much smaller volume of intercepted material is then selected to be read, looked at or listened to by persons. The intercepted material so selected must be certified (in the Secretary of State's certificate) as material 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 any 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)