No. 20-1191

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

WIKIMEDIA FOUNDATION,

Plaintiff–Appellant,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants–Appellees.

On Appeal from the United States District Court
for the District of Maryland at Baltimore

JOINT APPENDIX—VOLUME 3 OF 7 (JA1791–JA2352)

H. Thomas Byron III
Joseph Busa
Michael Shih
U.S. DEPARTMENT OF JUSTICE
950 Pennsylvania Ave. NW
Washington, DC 20530
Phone: (202) 616-5367
Fax: (202) 307-2551
h.thomas.byron@usdoj.gov

Counsel for Defendants–Appellees

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

Counsel for Plaintiff–Appellant
(Additional counsel on next page)

Alex Abdo
Jameel Jaffer
KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY
475 Riverside Drive, Suite 302
New York, NY 10115
Phone: (646) 745-8500
alex.abdo@knightcolumbia.org

Deborah A. Jeon
David R. Rocah
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., #350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838
rocah@aclu-md.org

Benjamin H. Kleine
COOLEY LLP
101 California Street, 5th Floor
San Francisco, CA 94111
Phone: (415) 693-2000
Fax: (415) 693-2222
bkleine@cooley.com

***Wikimedia Foundation v. National Security Agency, et al.*,**
No. 20-1191 (4th Cir.)

JOINT APPENDIX
Table of Contents

VOLUME 1

U.S. District Court for the District of Maryland, Docket Sheet,
Case No. 1:15-cv-00662 ..... JA0001

Plaintiff Wikimedia Foundation's Amended Complaint
(June 22, 2015), ECF No. 72 ..... JA0036

Exhibits to Wikimedia Foundation's Motion to Compel

Declaration of Patrick Toomey, Counsel for Wikimedia Foundation
(Mar. 26, 2018), ECF No. 125-3 ..... JA0096

Exhibit 1: Chart Identifying Discovery Requests at Issue on
Wikimedia Foundation's Motion to Compel,
ECF No. 125-4..... JA0101

Exhibit 2: Wikimedia Foundation's Requests for Admission
and attachments (Nov. 7, 2017), ECF No. 125-5..... JA0118

Exhibits to Defendants' Opposition to Wikimedia Foundation's Motion to Compel

Declaration of Daniel R. Coats, Director of National Intelligence
(Apr. 28, 2018), ECF No. 138-2..... JA0170

Declaration of Lauren L. Bernick, Senior Associate Civil Liberties
Protection Officer in the Office of Civil Liberties, Privacy, and
Transparency at the Office of the Director of National Intelligence
(Apr. 28, 2018), ECF No. 138-3..... JA0190

Notice of Filing Unclassified & Redacted Version of the Declaration of George C. Barnes, Deputy Director of the NSA (May 11, 2018), ECF No. 141 ..... JA0199

Unclassified & Redacted Version of the Declaration of George C. Barnes, Deputy Director of the NSA (May 11, 2018), ECF No. 141-1 ..... JA0201

Exhibits to Wikimedia Foundation's Reply in Support of Its Motion to Compel

Declaration of Ashley Gorski, Counsel for Wikimedia Foundation (May 18, 2018), ECF No. 143-1 ..... JA0270

Exhibit 1: Chart Identifying Deposition Questions at Issue on Wikimedia Foundation's Motion to Compel, ECF No. 143-2 ..... JA0272

Exhibit 2: Transcript of Deposition of NSA's Designated Witness, Rebecca J. Richards, Pursuant to Fed. R. Civ. P. 30(b)(6) (Apr. 16, 2018), ECF No. 143-3 ..... JA0286

Opinion & Order Denying Wikimedia Foundation's Motion to Compel

Memorandum Opinion (Aug. 20, 2018), ECF No. 150 ..... JA0689

Order Denying Plaintiff's Motion to Compel Discovery Responses & Deposition Testimony (Aug. 20, 2018), ECF No. 151 ..... JA0716

Exhibits to Defendants' Motion for Summary Judgment

Declaration of Henning Schulzrinne, Julian Clarence Levi Professor of Computer Science at Columbia University (Nov. 13, 2018), ECF No. 164-4 ..... JA0719

Declaration of James Gilligan, Counsel for Defendants (Nov. 13, 2018), ECF No. 164-5 ..... JA0818

Exhibit 3: Wikimedia Foundation's Amended and Supplemental Responses and Objections to NSA's First Set of Interrogatories (Mar. 23, 2018), ECF No. 164-6 ..... JA0821

Exhibit 4: Wikimedia Foundation's Amended Responses and Objections to ODNI's Interrogatory No. 19 (Apr. 6, 2018), including Technical Statistics Chart, ECF No. 164-7 ..... JA0861

Exhibit 5: Wikimedia Foundation's Responses and Objections to NSA's First Set of Interrogatories (Jan. 11, 2018), ECF No. 164-8..... JA0876

VOLUME 2

Exhibits to Wikimedia Foundation's Opposition to Defendants' Motion for Summary Judgment

Declaration of Scott Bradner, Former Senior Technology Consultant for the Harvard University Chief Technology Officer (Dec. 18, 2018), ECF No. 168-2 ..... JA0920

Appendices A through Z to Declaration of Scott Bradner (Dec. 18, 2018), ECF Nos. 168-3 to 168-4 ..... JA1067

VOLUME 3

Exhibits to Wikimedia Foundation's Opposition to Defendants' Motion for Summary Judgment (Cont'd)

Appendices AA through FF to Declaration of Scott Bradner (Dec. 18, 2020), ECF No. 168-5 ..... JA1791

Declaration of Jonathon Penney, Associate Professor at the Schulich School of Law and Director of the Law & Technology Institute at Dalhousie University (Dec. 18, 2018), ECF No. 168-6 ..... JA2151

Declaration of Michelle Paulson, Former Legal Director and Interim General Counsel for Wikimedia Foundation (Dec. 18, 2018), ECF No. 168-7 ..... JA2218

Declaration of James Alexander, Former Manager for Trust and Safety and Former Legal and Community Advocacy Manager at Wikimedia Foundation (Dec. 18, 2018), ECF No. 168-8 ..... JA2244

Declaration of Tilman Bayer, Senior Analyst for Wikimedia Foundation Product Analytics Team (Dec. 18, 2018), ECF No. 168-9 ..... JA2253

Declaration of Emily Temple-Wood (Dec. 18, 2018), ECF No. 168-10 ..... JA2268

Declaration of Patrick Toomey, Counsel for Wikimedia Foundation (Dec. 18, 2018), ECF No. 168-11 ..... JA2278

Exhibit 8: Wikimedia-hosted email list discussing NSA slide with Wikimedia logo, from July to August 2013, ECF No. 168-12 ..... JA2283

Exhibit 9: Wikimedia "Talk page" discussing its non-public information policy, from September to December 2013, ECF No. 168-13 ..... JA2305

Exhibit 10: "OTRS" ticket showing Wikimedia user requesting Tor permissions in September 2013, ECF No. 168-14 ..... JA2349

VOLUME 4

Exhibits to Wikimedia Foundation's Opposition to Defendants' Motion for Summary Judgment (Cont'd)

Exhibit 11: Wikimedia webpage showing Wikimedia user requesting Tor permissions in September 2017, ECF No. 168-15 ..... JA2353

Exhibit 12: Wikimedia document compiling German-user-

community appeal concerning privacy in 2013,
ECF No. 168-16 ..... JA2357

Exhibit 13: Wikimedia "Talk page" discussing NSA
surveillance from June to December 2013,
ECF No. 168-17 ..... JA2363

Exhibit 14: Wikimedia Technical Statistics Chart & Supporting
Exhibits A-G, ECF No. 168-18 ..... JA2396

Exhibit 15: Privacy & Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* (July 2014), ECF No. 168-19 ..... JA2434

Exhibit 16: FISC Memorandum Opinion, [*Redacted*], 2011 WL
10945618 (Oct. 3, 2011), ECF No. 168-20 ..... JA2631

Exhibit 17: Office of the Director of National Intelligence, *DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 702 of FISA* (Aug. 21, 2013),
ECF No. 168-21 ..... JA2717

Exhibit 18: Defendant NSA's Objections and Responses to
Plaintiff's First Set of Interrogatories (Dec. 22, 2017),
ECF No. 168-22 ..... JA2721

Exhibit 19: FISC Submission, *Clarification of National Security Agency's Upstream Collection Pursuant to Section 702 of FISA*
(May 2, 2011), ECF No. 168-23 ..... JA2743

Exhibit 20: Office of the Director of National Intelligence,
Statistical Transparency Report Regarding Use of National Security Authorities, Calendar Year 2017 (Apr. 2018),
ECF No. 168-24 ..... JA2748

Exhibit 21: FISC Memorandum Opinion & Order
(Apr. 26, 2017), ECF No. 168-25 ..... JA2790

VOLUME 5

Exhibits to Wikimedia Foundation's Opposition to Defendants' Motion for Summary Judgment (Cont'd)

Exhibit 22: FISC Submission, *Government's Response to the Court's Briefing Order of May 9, 2011* (June 1, 2011), ECF No. 168-26 ..... JA2890

Exhibit 23: *Big Brother Watch & Others v. United Kingdom*, App. Nos. 58170/13, 62322/14, 24960/15, Eur. Ct. H.R. (2018), ECF No. 168-27 ..... JA2932

Exhibit 24: NSA Director of Civil Liberties & Privacy Office, *NSA's Implementation of FISA Section 702* (Apr. 16, 2014), ECF No. 168-28 ..... JA3145

Exhibit 25: *Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (EINSTEIN 2.0)*, 33 Op. O.L.C. 1 (Jan. 9, 2009), ECF No. 168-29 ..... JA3157

Exhibit 26: Minimization Procedures Used by the NSA in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of FISA (July 2014), ECF No. 168-30 ..... JA3193

Exhibit 27: Glenn Greenwald, *XKeyscore: NSA Tool Collects "Nearly Everything a User Does on the Internet,"* Guardian, July 31, 2013, ECF No. 168-31 ..... JA3209

Exhibit 28: NSA slide, excerpted from Exhibit 27 (Greenwald, *XKeyscore: NSA Tool Collects "Nearly Everything a User Does on the Internet"*), ECF No. 168-32 ..... JA3220

Exhibit 29: Morgan Marquis-Boire, et al., *XKEYSCORE: NSA's Google for the World's Private Communications*, Intercept, July 1, 2015, ECF No. 168-33 ..... JA3222

Exhibit 30: NSA slide deck, *XKEYSCORE for Counter-CNE*, published in The Intercept on July 1, 2015, ECF No. 168-34 ... JA3237

Exhibit 31: Wikimedia, *Founding Principles* (accessed Mar. 14, 2018), ECF No. 168-35 ..... JA3259

Exhibit 32: Yana Welinder, *Opposing Mass Surveillance on the Internet*, Wikimedia Blog (May 9, 2014), ECF No. 168-36 ..... JA3262

Exhibit 33: Wikimedia Public Policy, *Privacy* (accessed Mar. 14, 2018), ECF No. 168-37 ..... JA3266

Exhibit 34: Wikipedia, *Sock Puppetry* (accessed Mar. 14, 2018), ECF No. 168-38 ..... JA3273

Exhibit 35: Wikimedia, *Privacy Policy* (accessed Feb. 14, 2018), ECF No. 168-39 ..... JA3286

Exhibit 36: Ryan Lane, *The Future of HTTPS on Wikimedia Projects*, Wikimedia Blog (Aug. 1, 2013), ECF No. 168-40 ..... JA3311

Exhibit 37: Yana Welinder, et al., *Securing Access to Wikimedia Sites with HTTPS*, Wikimedia Blog (June 12, 2015), ECF No. 168-41 ..... JA3317

Exhibit 38: Wikimedia email describing Tech/Ops goals and the importance of HTTPS (May 23, 2014), ECF No. 168-42 .... JA3325

Exhibit 39: Wikimedia document discussing IPsec implementation, including July 8, 2013 statement from a Wikimedia engineer, ECF No. 168-43 ..... JA3328

Exhibit 40: Wikimedia job posting for Traffic Security Engineer (accessed Feb. 8, 2018), ECF No. 168-44 ..... JA3364

Exhibit 41: Michelle Paulson, *A Proposal for Wikimedia's New Privacy Policy and Data Retention Guidelines*, Wikimedia Blog (Feb. 14, 2014), ECF No. 168-45 ..... JA3367

Exhibit 42: Wikimedia's Supplemental Exhibit C in response

to NSA Interrogatory No. 8 (volume of HTTP border-crossing communications by country), ECF No. 168-46 ..... JA3375

Exhibit 43: Wikimedia's Supplemental Exhibit D in response to NSA Interrogatory No. 8 (volume of HTTPS border-crossing communications by country), ECF No. 168-47 ..... JA3388

Exhibit 44: Wikimedia analytics document showing monthly unique visitors to Wikimedia by region, from December 2007 to May 2015, ECF No. 168-48 ..... JA3400

Exhibit 45: Press Release, NSA, *NSA Stops Certain Section 702 "Upstream" Activities*, Apr. 28, 2017, ECF No. 168-49 ..... JA3404

VOLUME 6

Exhibits to Defendants' Reply in Support of Their Motion for Summary Judgment

Second Declaration of Henning Schulzrinne, Julian Clarence Levi Professor of Computer Science at Columbia University (Feb. 15, 2019), ECF No. 178-2 ..... JA3407

Declaration of Alan J. Salzberg, Principal of Salt Hill Statistical Consulting (Feb. 15, 2019), ECF No. 178-3 ..... JA3452

Second Declaration of James Gilligan, Counsel for Defendants (Feb. 15, 2019), ECF No. 178-4 ..... JA3725

Exhibit 9: Wikimedia Foundation's Responses and Objections to DOJ's First Set of Interrogatories (Jan. 11, 2018), ECF No. 178-5 ..... JA3728

Exhibit 10: Relevant Portions of the Deposition of James Alexander, Wikimedia Foundation witness taken pursuant to Fed. R. Evid. 30(b)(6), ECF No. 178-6 ..... JA3761

Exhibit 11: Relevant Portions of the Deposition of Michelle

Paulson, Wikimedia Foundation witness taken pursuant to Fed. R. Evid. 30(b)(6), ECF No. 178-7 ..... JA3777

Exhibit 12: Wikimedia Foundation, *Securing access to Wikimedia sites with HTTPS*, June 12, 2015 (WIKI0007108-7114), ECF No. 178-8 ..... JA3791

Exhibit 13: Wikipedia: Village pump (technical)/Archive 138 (WIKI0006872-6938), ECF No. 178-9 ..... JA3800

Exhibit 14: Jimmy Wales and Lila Tretikov, "Stop Spying on Wikimedia Users," N.Y. Times, Mar. 10, 2015, ECF No. 178-10 ..... JA3869

Exhibit 15: Wikimedia Foundation, *Wikimedia v. NSA: Wikimedia Foundation files suit against NSA to challenge upstream mass surveillance*, Mar. 10, 2015, ECF No. 178-11 ..... JA3873

VOLUME 7

Exhibits to Wikimedia Foundation's Sur-reply in Opposition to Defendants' Motion for Summary Judgment

Second Declaration of Scott Bradner, Former Senior Technology Consultant for the Harvard University Chief Technology Officer (Mar. 8, 2019), ECF No. 181-1 ..... JA3879

Second Declaration of Jonathon Penney, Associate Professor at the Schulich School of Law and Director of the Law & Technology Institute at Dalhousie University (Mar. 8, 2019), ECF No. 181-2 ..... JA3940

Second Declaration of Michelle Paulson, Former Legal Director and Interim General Counsel for Wikimedia Foundation (Mar. 8, 2019), ECF No. 181-3 ..... JA4006

Second Declaration of Tilman Bayer, Senior Analyst for Wikimedia Foundation Product Analytics Team (Mar. 8, 2019), ECF No. 181-4 ..... JA4012

Second Declaration of Emily Temple-Wood (Mar. 8, 2019),
ECF No. 181-5 ..... JA4015

Exhibits to Defendants' Sur-reply in Support of Their Motion for Summary Judgment

Third Declaration of Henning Schulzrinne, Julian Clarence Levi Professor of Computer Science at Columbia University
(Mar. 22, 2019), ECF No. 182-2 ..... JA4019

Second Declaration of Alan J. Salzberg, Principal of Salt Hill Statistical Consulting (Mar. 22, 2019), ECF No. 182-3 ..... JA4048

Opinion & Order Granting Defendants' Motion for Summary Judgment

Memorandum Opinion (Dec. 16, 2019), ECF No. 188 ..... JA4073

Order Granting Defendants' Motion for Summary Judgment
(Dec. 16, 2019), ECF No. 189 ..... JA4123

Wikimedia Foundation's Notice of Appeal

Notice of Appeal (Feb. 14, 2020), ECF No. 191 ..... JA4124

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

This document was also filed as ECF No. 164-7 and can be found in this Joint Appendix at JA0861.

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

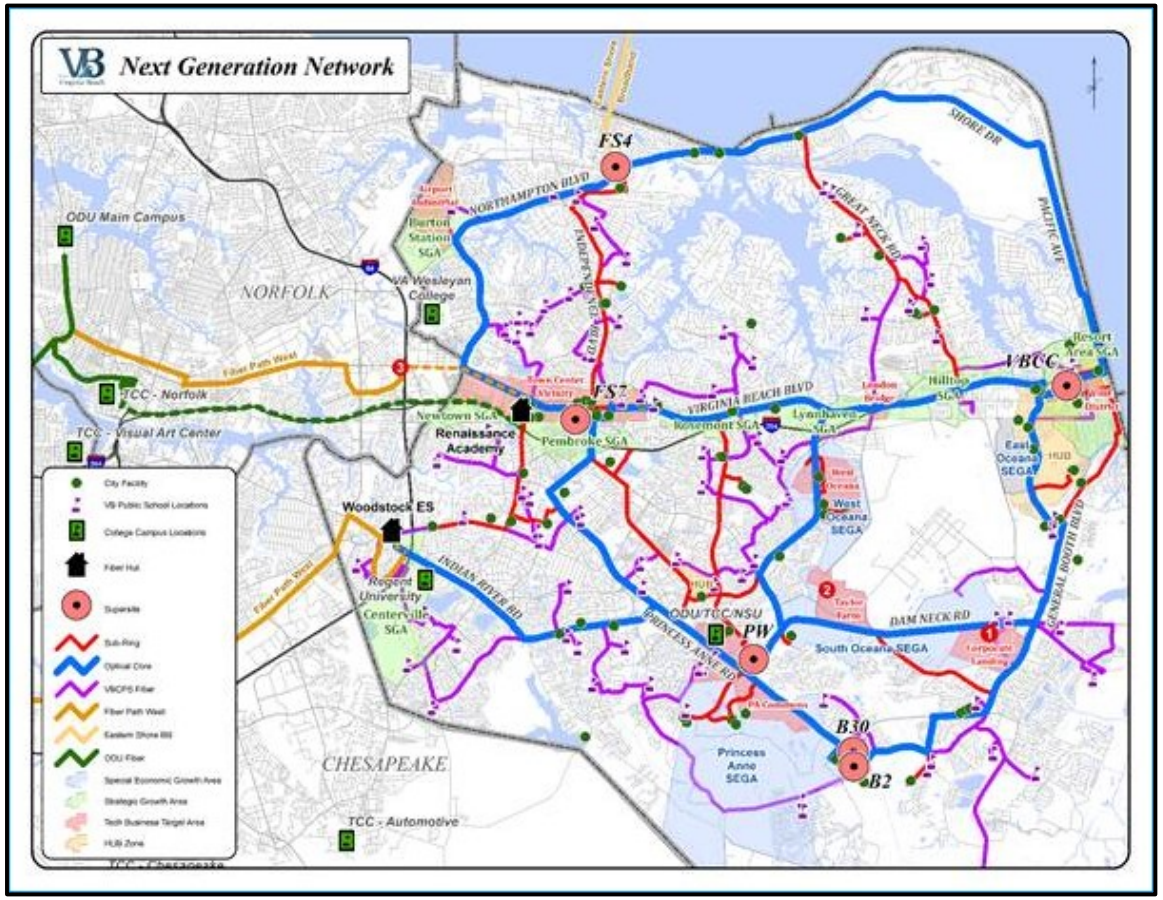
- **CBG Communications**
  - Telecommunications and cable television consulting firm that conducted both residential and business broadband surveys to gauge the community's need for broadband services.

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

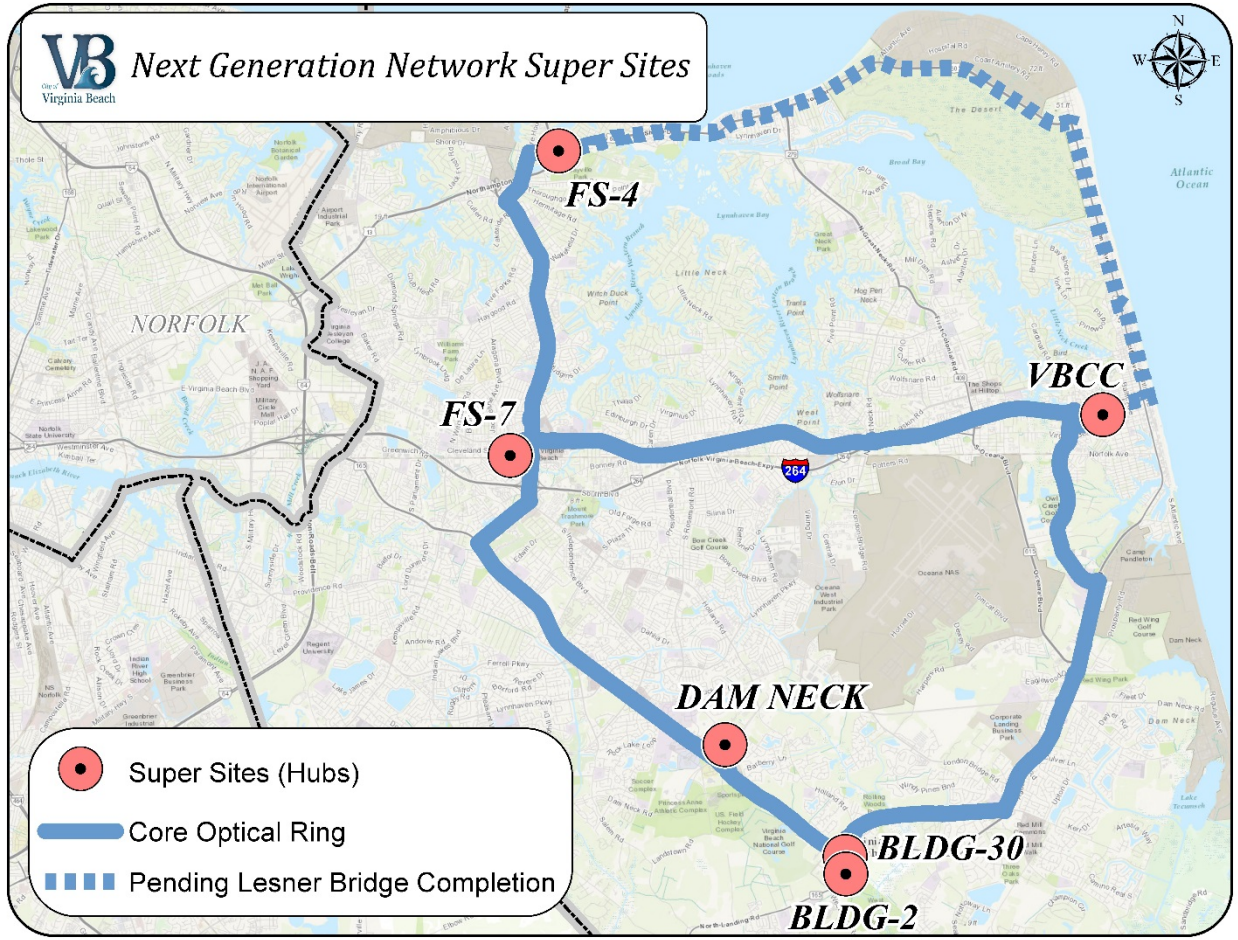
- **CTC Technology & Energy**
  - An independent communications and IT engineering consulting firm that assisted with developing middle mile leasing strategies.

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

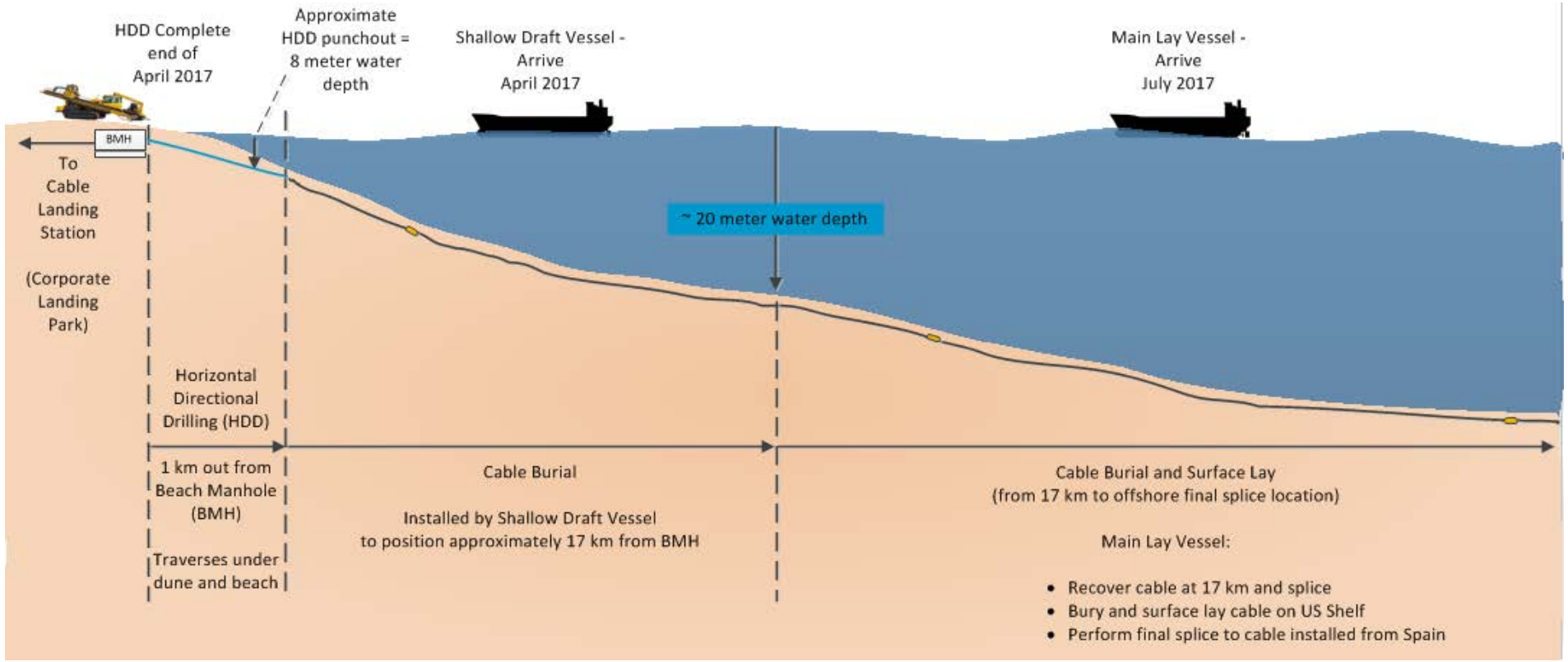


- Total of 6 Optical/Super Sites (Phase 0) and
- 54 Remote Locations (Phases 1 through 4)
- Construction Completion Dates:
  - Phase 0 – 06/24/2016
  - Phase 1 – 10/18/2016
  - Phase 2 – 04/07/2017
  - Phase 3 – 04/28/2017
  - Phase 4 – 06/15/2017
- NGN Go Live Date – Dec, 2017

Transoceanic Subsea Fiber Cables

MAREA Cable – From beach to manhole

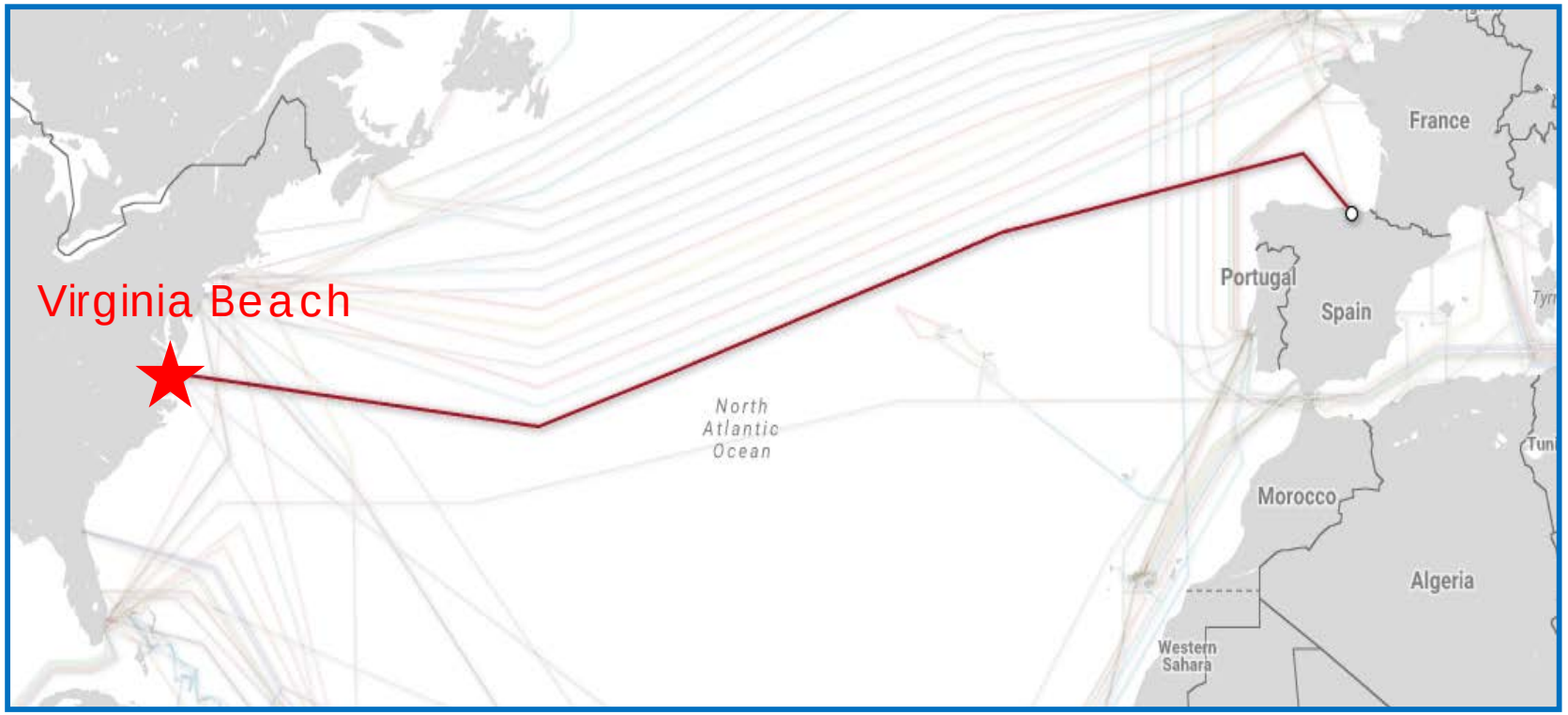
- **Oceanic** Infrastructure connection of subsea cable
  - Will connect sub-sea cable to off-shore duct duckbill flap (4 conduits for the MAREA/BRUSA beach manhole)
  - Clear in (ships check in port)
    - (shallow draft vessel) April 7 – 14, 2017
    - (main lay vessel) July 19 – Aug 15, 2017
  - Operational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



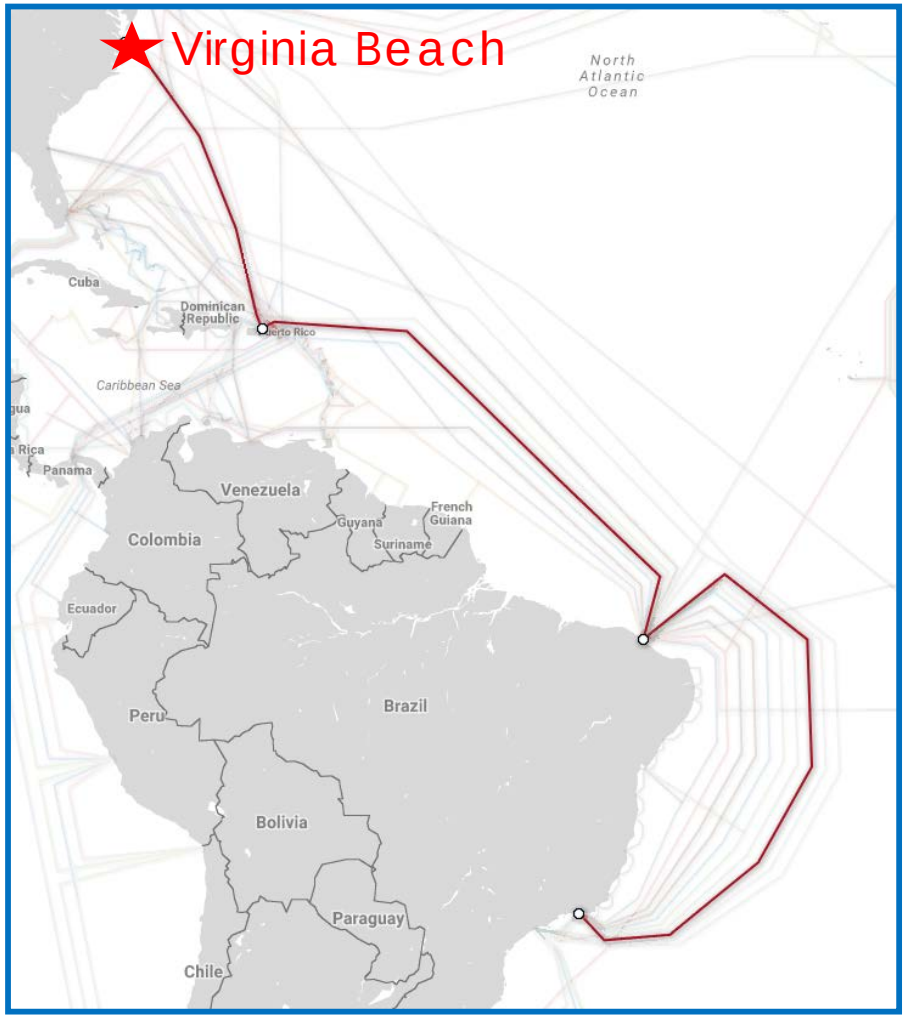
- Led by **Microsoft and Facebook, MAREA will be the highest-capacity subsea cable to ever cross the Atlantic**
- The new **6,600 km submarine cable system** will connect **Virginia Beach, Virginia to Bilbao, Spain**
- This new southern **route will provide greater diversity of connections & enhanced 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

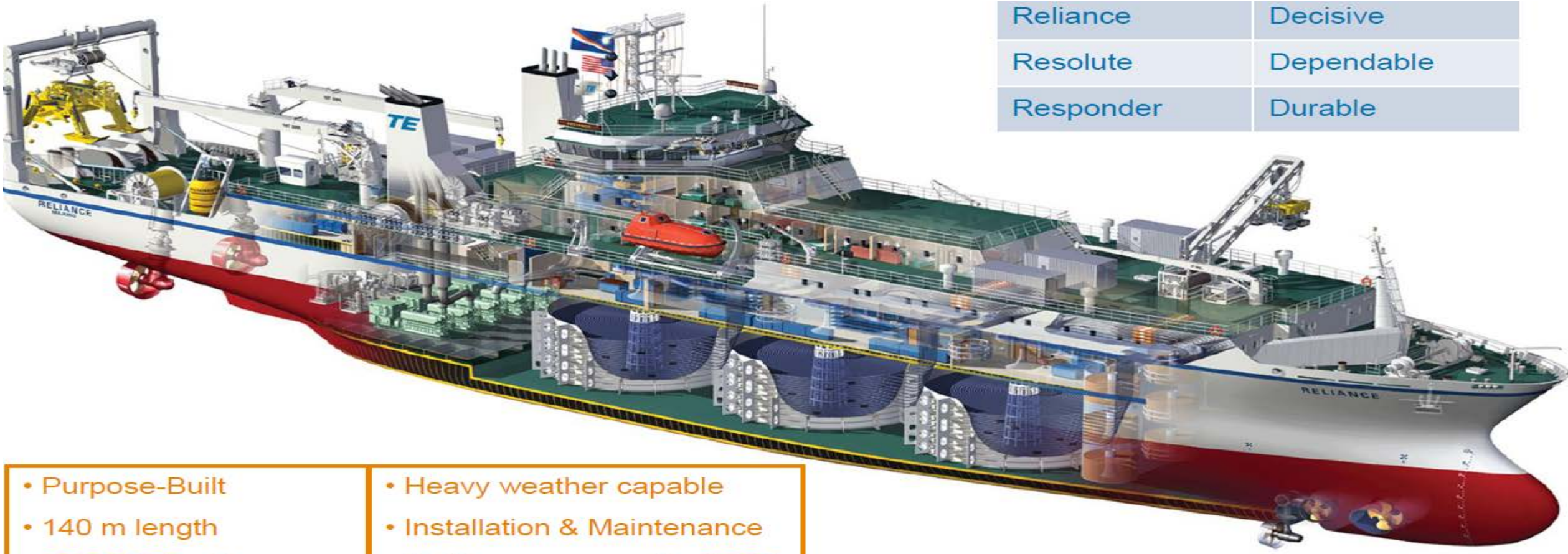


BRUSA Cable and Conduit Installation: **June 2018**
(dates per Telefonica)

- 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

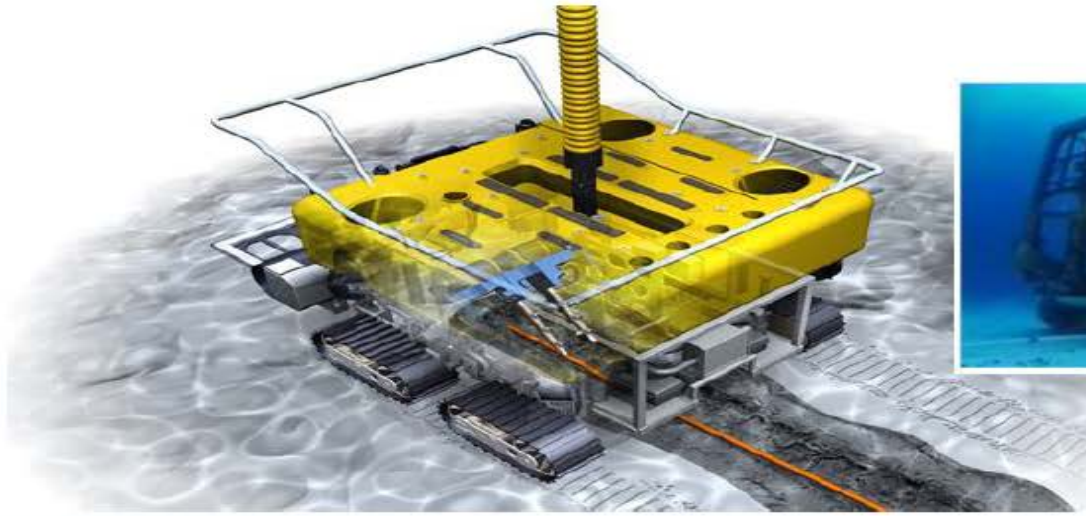


- Purpose-Built
- 140 m length
- 5,500 MT cable cap.
- 84 persons
- 60+ days endurance

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

JA1874

Transoceanic Subsea Fiber Cables
Remotely Operated Vehicles (ROV)



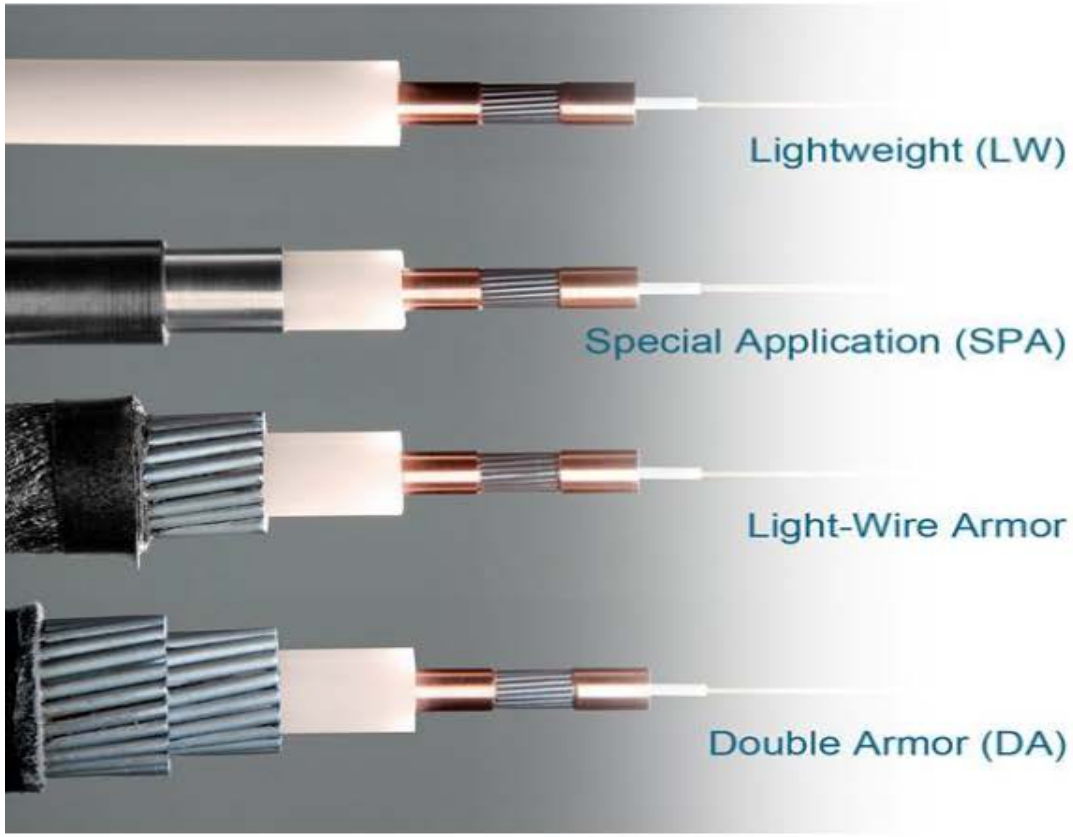






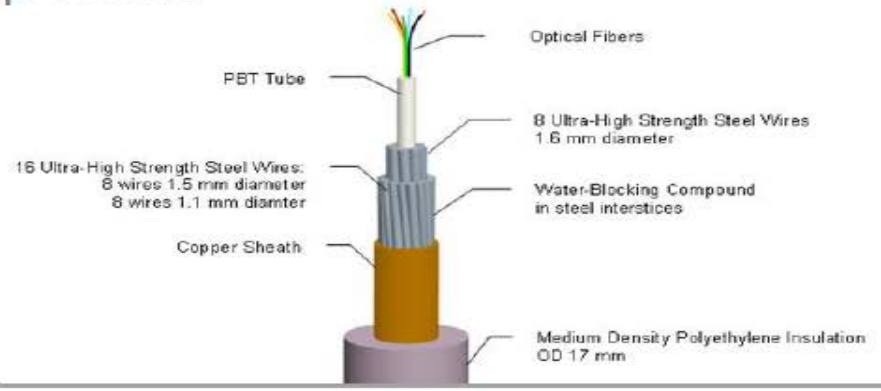


Transoceanic Subsea Fiber Cables



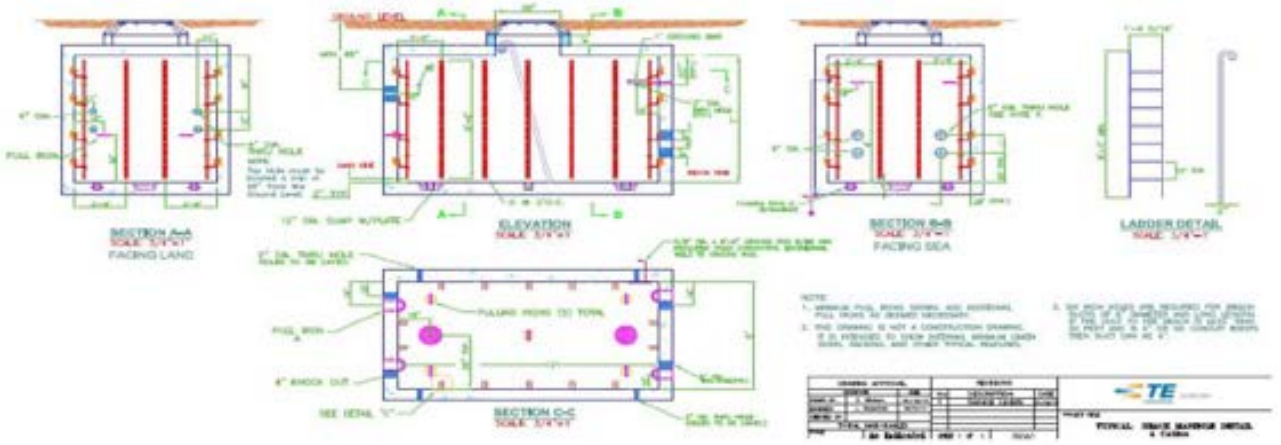
Undersea cables…

- 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



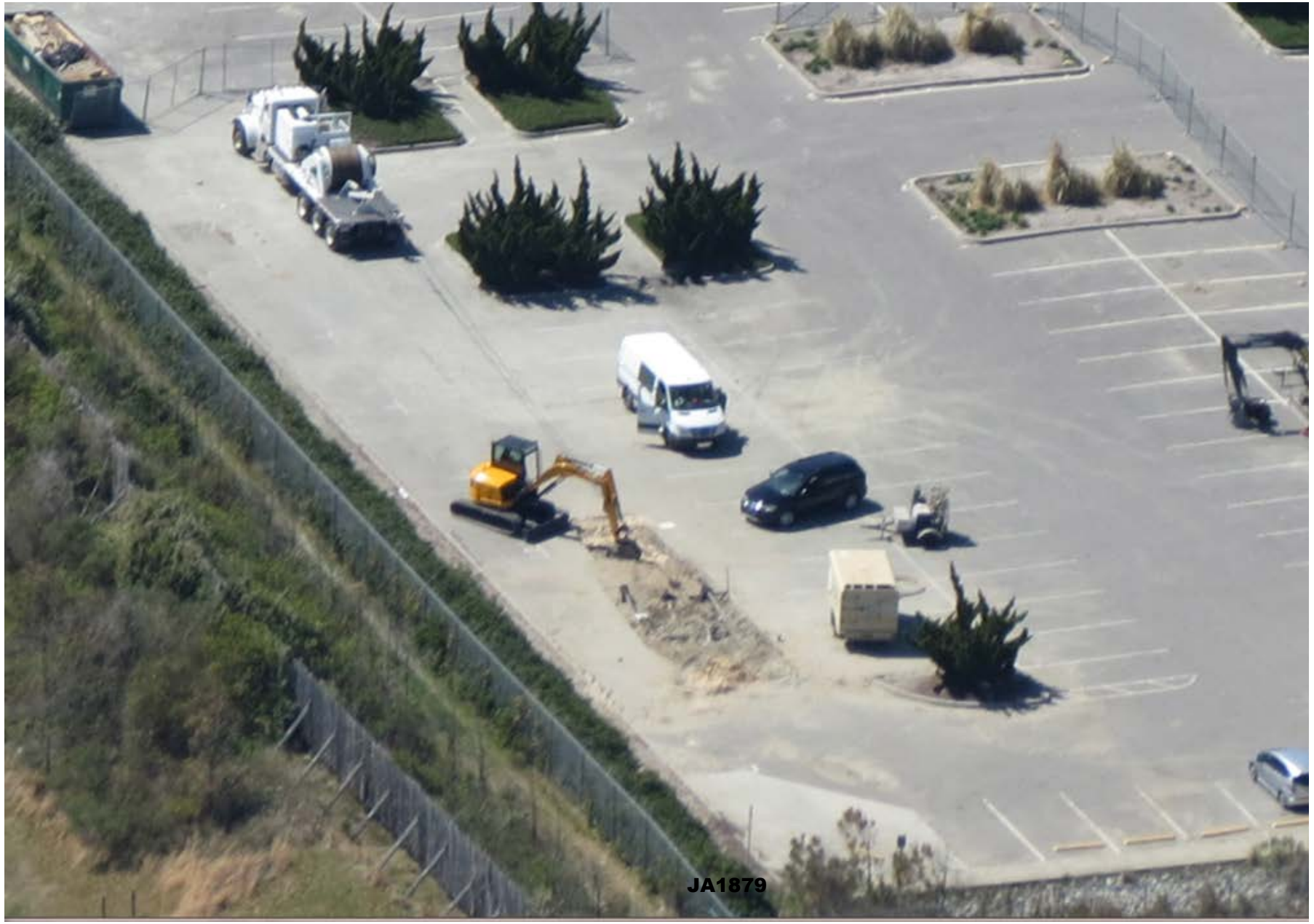


- **2 BMH's planned**
- **Typical BMH Design: 12' L x 6' W x 7' H**
- **Buried (below ground level) within the parking lot, with corresponding buried ocean ground bed anodes**
- **No Significant impact to the long-term functionality of the parking lot**

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

This document was also filed as ECF No. 168-27 and can be found in this Joint Appendix at JA2932.

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 - *see, 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 6-28

Part 1 - The Facts 29
- *i. The Prism/Upstream complaint*
  - *a. The Prism/Upstream Programmes* 30-37
  - *b. Receipt of material from a foreign state* 37-40
- *ii. The "Tempora" complaint*
  - *a. The nature of s.8(4) interception* 40-45
  - *b. The rationale for and utility of s.8(4) interception* 45-51
  - *c. Internal and external communications* 51-54
- *iii. Proceedings in the IPT* 54-59

Part 2 - Domestic Law and Practice
- *i. The Intelligence Sharing Regime* 59-73
- *ii. The s.8(4) Regime* 73-103

Part 3 - Response to the Grounds
- *i. The Intelligence Sharing Regime*
  - *a. The Applicants do not have victim status* 103-107
  - *b. Article 8 -*
    - *(i) The Regime is "in accordance with the law"* 107-120
    - *(ii) The necessity test* 121

- *ii. The s.8(4) Regime*
  - *a. Victim status* 121
  - *b. Article 8*
    - *(i) Preliminary points* 121-132
    - *(ii) The Regime is "in accordance with the law"* 132-133
      - *Foreseeability: interception of communications* 133-143
      - *Foreseeability: acquisition of communications data* 143-147
      - *Further points on foreseeability/accessibility* 147-155
    - *(iii) Necessity* 155-161
    - *(iv) Specific criticisms of IPT's Third Judgment* 161-165

- *iii. The Applicants' status as NGOs:*
  - *a. Article 8* 166
  - *b. Article 10* 166-180

- *iv. Article 6*
  - *a. The rights at issue are not "civil rights"* 180-184
  - *b. Were the IPT proceedings compliant with Article 6?* 184-199

- *v. Article 14* 199-204

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 any 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 not 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 in principle 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 obligation under a mutual assistance agreement. They do not apply to the discretionary 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 all customer data for a period of not less than 6 months, and up to 2 years, so that it could be made available to law enforcement authorities. The Directive contained no substantive safeguards at all circumscribing access to or use of that communications data.

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 <u>cannot</u> be used (in combination with other information / intelligence) to discover *e.g.* that a woman of no intelligence interest may be planning an abortion. 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 should be relatively rare. So it is practicable and proportionate for the Secretary of State to

consider each such instance, and (if appropriate) certify that this is indeed necessary under s. 16(3) RIPA:

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

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)

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

Plaintiff's Exhibit 2

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION,

Plaintiff,

v.

NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE, *et al.*,

Defendants.

No. 1:15-cv-00662-TSE

DECLARATION OF JONATHON PENNEY

TABLE OF CONTENTS

I. Qualifications 1
II. Assignment 3
III. Summary of Opinions 4
IV. Overview of Chilling Effects Theory & Supporting Empirical Evidence for Surveillance Related Chill Online 4
V. Wikipedia Study—Design, Method, and Results 10
A. Design 11
i. Intervention Selection 12
ii. Data Selection 14
iii. Data Collection 16
B. Method of Analysis 17
C. Results 19
i. First Set of Results: 48 Terrorism Wikipedia Article Group 19
ii. Second Set of Results: 47 Wikipedia Terrorism Article Group (Without Hamas Outlier) 21
iii. Third Set of Results: 31 Most Privacy-Sensitive Wikipedia Terrorism Article Group 23
iv. Comparator Wikipedia Article Groups 25
VI. Conclusion 28

I. QUALIFICATIONS

1. I am an Associate Professor at the Schulich School of Law and Director of the Law & Technology Institute at Dalhousie University, located in Halifax, Canada. I submit this declaration in support of Plaintiff Wikimedia Foundation's ("Wikimedia's") Opposition to Defendants' Motion for Summary Judgment. Unless otherwise stated, I have personal knowledge of the facts herein.

2. I am a legal academic and social scientist. I hold a DPhil (Ph.D.) in Information, Communication, and the Social Sciences and an M.S.T. in Legal Research from the University of Oxford, as well as an L.L.M. from Columbia Law School, and a J.D. and B.A. from Dalhousie University.

3. I have extensive experience in the scientific study of social phenomena, specifically as it relates to online behavior. During my doctoral studies at Oxford, I received substantial training in empirical, statistical, and social science methods. In addition to my professorship, I also hold appointments at leading research centers in my field. I am currently a Research Fellow at the Citizen Lab, located at the University of Toronto's Munk School of Global Affairs and Public Policy; a Research Associate of Princeton's Center for Information Technology Policy and the Civil Servant Project at the Massachusetts Institute of Technology's Media Lab; and was formerly a Berkman Fellow and Research Affiliate at the Berkman Klein Center for Internet & Society at Harvard University.

4. I have a deep understanding of "chilling effects" theory—the idea that laws, surveillance, or other regulatory actions may "chill" or deter individuals from exercising their rights or freedoms. A central focus of my doctoral dissertation at Oxford was the study of Internet surveillance-related chilling effects. I collected and analyzed data that showed increased public

awareness of National Security Agency ("NSA") surveillance practices resulted in a reduction of privacy-sensitive Wikipedia article page views, and concluded this reduction was evidence of a statistically significant "chilling effect."

5. My doctoral dissertation, which included this Wikipedia "chilling effects" study, was peer reviewed by two examiners for my doctoral thesis defense at the University of Oxford in November 2015. The examiners were Urs Gasser, Professor at Harvard Law School and Executive Director of Harvard University's Berkman Klein Center for Internet and Society, and Joss Wright, Senior Research Fellow at the Oxford Internet Institute, University of Oxford, and a Turing Fellow at the Alan Turing Institute, the United Kingdom's national institute for data science and artificial intelligence. The thesis, which included the study, was successfully defended and accepted with no corrections. The study was also formally peer reviewed, and a draft paper based on it accepted for presentation, by members of the Program Committee for the Inaugural Society for Empirical Legal Studies (SELS) Global Junior Empirical Legal Scholars Workshop in December 2015. The Program Committee reviewed all submissions and selected the best papers for presentation at the workshop. The Program Committee included some of the leading empirical legal scholars internationally, including David Abrams, Professor of Law, Business Economics, and Public Policy at University of Pennsylvania Law; Bernie Black, the Nicholas D. Chabraja Professor at Northwestern University School of Law; Valarie Hans, Professor at Cornell Law School; and Eyal Zamir, Augusto Levi Professor of Commercial Law and Director of the Center for Empirical Studies of Decision Making and the Law at Hebrew University.

6. Informally, the study was also peer reviewed by computational social scientist Nathan Matias in May 2016, who at the time was a doctoral candidate at the Massachusetts Institute of Technology's Media Lab and is now a Post-Doctoral Research Associate at Princeton University,

cross-appointed in Princeton's Psychology Department, Sociology Department, and the Center for Information Technology Policy. In addition, Matthew Salganik, Professor in the Department of Sociology at Princeton University, has reviewed the study, using it as part of course materials for his class, "Computational Social Science: Social Research in the Digital Age," at Princeton University's Sociology Department. He has also cited the study multiple times in his leading text on computational social science research and methods.[1]

7. The study was also informally peer reviewed via numerous presentations to faculty, academic researchers, graduate students, and a range of other experts in 2015 and 2016, including Harvard University's Berkman Klein Center for Internet and Society in May 2015 and April 2016; and the 5th Annual Workshop on Free and Open Communications on the Internet (FOCI) Workshop, USENIX Security Symposium, Advanced Computing Systems Association (ACSA), Washington, D.C. in August 2015.

8. In 2016, I published the findings from my doctoral research in the *Berkeley Technology Law Journal*. I have also published other research on chilling effects and online privacy in peer-reviewed data science and policy journals. My statement of qualifications, including my professional curriculum vitae and list of publications, is attached as Appendix B.

II. ASSIGNMENT

9. Wikimedia has retained me to provide expert consultation, analyses, and testimony in the lawsuit *Wikimedia Foundation v. National Security Agency, et al.*, No. 1:15-cv-00662-TSE (D. Md.). My assignment is to provide opinions on the chilling effects associated with "Upstream" Internet surveillance conducted by the Defendant National Security Agency ("NSA"). Neither

[1] *See* MATTHEW SALGANIK, BIT BY BIT: SOCIAL RESEARCH IN THE DIGITAL AGE (2017).

Wikimedia nor anyone else is compensating me for this work, and my participation is not dependent on the opinions provided or the outcome of the case.

III. SUMMARY OF OPINIONS

10. Based on the empirical evidence and my statistical analysis, I conclude that public awareness of NSA surveillance programs, including Upstream surveillance, which became widespread during the June 2013 Snowden disclosures, is highly likely to have had a large-scale chilling effect on Wikipedia users.

11. I arrive at this conclusion based on (1) the statistically significant and substantial drop in view counts immediately following June 2013 for Wikipedia articles that would likely raise privacy concerns for users aware of NSA Internet surveillance; (2) the statistically significant trend reversal in monthly views for those articles after June 2013, which indicates a sustained impact on viewership that did not course correct after this revelation; and (3) the lack of comparable statistically significant reductions and reversals in monthly article views for comparator Wikipedia articles over the same time period.

IV. OVERVIEW OF CHILLING EFFECTS THEORY & SUPPORTING EMPIRICAL EVIDENCE FOR SURVEILLANCE RELATED CHILL ONLINE

12. Chilling effects theory posits that government surveillance can harm individuals by "chilling" or deterring them from exercising their rights and freedoms out of fear of legal punishment, social sanction, or to avoid invasions of privacy and reputational risks. There is an extensive body of legal scholarship establishing the underpinnings of chilling effects theory.[2]

[2] *See generally* Frederick Schauer, *Fear, Risk, and the First Amendment: Unraveling the "Chilling Effect,"* 58 B.U. L. REV. 685 (1978) (the leading academic account of chilling effects theory); Daniel Solove, *A Taxonomy of Privacy*, 154 U. PENN. L. REV. 477 (2006) (analyzing theory in the context of modern surveillance practices and data gathering, focusing on how government surveillance of online activities creates a broader atmosphere of conformity and self-censorship).

13. Some social science research has indicated that self-reported or expressed concerns about privacy do not necessarily reflect people's actual behavior online, a phenomenon sometimes referred to as the "privacy paradox."[3] However, especially in recent years, empirical studies have tested and confirmed the tenets of chilling effects theory as they apply to online behavior, including specifically as it relates to online government surveillance.

14. Social science research and empirical studies have been conducted that demonstrate online behavior is chilled as a result of government surveillance. Importantly, multiple studies confirm specifically that public awareness surrounding NSA surveillance activities, including Upstream surveillance, created a chilling effect online. *See also infra* Part V.A.i (establishing significance of public awareness and shock created by media coverage of the Snowden disclosures).

15. A Massachusetts Institute of Technology (MIT) study on Google search traffic by Alex Marthews and Catherine Tucker, later published in 2017 as a peer reviewed chapter in the Cambridge University Handbook on Surveillance Law, found a statistically significant 4% reduction in Google searches after the June 2013 Snowden disclosures for certain search terms that would raise privacy concerns for Internet users aware of NSA surveillance online.[4] This finding, that awareness of online surveillance chilled Internet users from searching for certain topics and content, strongly supports the conclusions I draw herein. It also provides additional evidence that

[3] *See* Spyros Kokolakis, *Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon*, COMPUTERS & SOC'Y 1 (2015) (providing a comprehensive explanation and review of "information privacy paradox" literature).

[4] Alex Marthews & Catherine Tucker, *Government Surveillance and Internet Search Behavior*, *in* CAMBRIDGE UNIVERSITY HANDBOOK ON SURVEILLANCE LAW (David Gray et al. eds., 2017).

Internet users were generally aware of NSA surveillance starting as of June 2013, and it impacted their online activities.

16. Elizabeth Stoycheff's 2016 experimental study, later published in a peer reviewed article entitled "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring," found that exposing participants to "terms of agreement," which reminded participants that their online activities could be subject to interception and surveillance, chilled those participants from expressing their political views, especially those participants who believed their political views were controversial or less popular.[5] Again, this chilling effect, due to awareness of online surveillance, is consistent with findings from my own observational study.

17. Andrea Forte et al.'s 2017 qualitative study on Wikipedia editors, published in a peer reviewed paper entitled "Privacy, Anonymity, and Perceived Risk in Open Collaboration: A Study of Tor Users and Wikipedians," found evidence that editors were chilled from certain activities on Wikipedia due to awareness of government surveillance.[6] For example, one Wikipedia editor stated that surveillance "has a chilling effect on the way that we do business and on the ability which Wikipedia has, [as] an enterprise, to continue. Because people are far less likely to engage with us, if they know that the American government is watching their every move." Another Wikipedia editor confirmed these chilling effects, stating, "for the Edward Snowden page, I have pulled myself away from adding sensitive contributions, like different references, because I thought the name may be traced back to me in some way." These findings are also consistent with my conclusions about chilling effects on Wikipedia use.

---

[5] Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93(2) JOURNALISM & MASS COMMUNICATION 296 (2017).

[6] Andrea Forte, Nazanin Andalibi, and Rachel Greenstadt, *Privacy, Anonymity, and Perceived Risk in Open Collaboration: A Study of Tor Users and Wikipedians*, in CSCW 1800 (2017).

18. A series of survey-based empirical studies of Americans published by PEW Research Center in 2013, 2014, and 2015 found people were chilled in their online activities due to their awareness of government surveillance programs after June 2013.[7] A Pew Research Center survey of 475 adult Americans conducted between November 26, 2014 and January 3, 2015, and published in a report entitled "Americans' Privacy Strategies Post-Snowden" in March 2015, found 87% of respondents were aware of "government surveillance programs to monitor phone use and internet use" due to the Snowden disclosures. Among that 87%, 34% had taken "at least one step to hide or shield their information from the government" such as changing privacy settings, using social media less, avoiding certain apps, speaking more in person than online, and avoiding using "certain terms in online communications." It also found 25% changed the patterns of their own use of various technological platforms "a great deal" or "somewhat" since the Snowden revelations. Similarly, a survey of 1,801 adults conducted between August 7-September 16, 2013, and published in a report entitled "Americans' Privacy Strategies Post-Snowden" in August 2014, found that survey respondents were less willing to discuss the "Snowden-NSA story" online "than they were in person" with 86% indicating they would speak about the story "in person" but only 42% would speak about it on social media. Again, a July 2013 survey of 1,002 American adults ages 18 and older, published in a report entitled "Anonymity, Privacy, and Security Online" in September 2013, found 86% tried to use the Internet in ways to minimize the visibility of their digital footprints, including 55% saying that had "used the internet in ways to

[7] KEITH N. HAMPTON ET AL., PEW RES. CTR., SOCIAL MEDIA AND THE 'SPIRAL OF SILENCE,' 4 (2014), http://www.pewinternet.org/files/2014/08/PI_Social networks and debate_082614.pdf; LEE RAINIE ET AL., PEW RES. INTERNET PROJECT, AMERICANS' PRIVACY STRATEGIES POST-SNOWDEN 4 (Mar. 16, 2015), http://www.pewinternet.org/files/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf; Lee Rainie et al., *Anonymity, Privacy, and Security Online*, Pew Res. Ctr. (2013), http://www.pewinternet.org/2013/09/05/anonymity privacy and security online.

avoid being observed or seen" by a range of people, groups, and institutions, including government and law enforcement. All of these studies are consistent with the results of my empirical study of Wikipedia page view traffic. They also critically support June 2013 as the initial date that people became aware of NSA surveillance activities, including Upstream surveillance.

19. A PEN American Center study of writers in 2013 and 2015 also found evidence of chilling effects associated with awareness of government surveillance after the Snowden revelations in June 2013.[8] The October 2013 survey of 520 American writers, later published in a report entitled "Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor" in November 2013, found that 28% of the writers surveyed had "curtailed or avoided" certain online activities due to "fear of surveillance" and another 12% "seriously considered" doing so; 24% "deliberately avoided certain topics in phone or email conversations," and another 9% have "seriously considered it"; and 16% have refrained from "conducting Internet searches or visiting websites on topics that may be considered controversial or suspicious," and another 12% have "seriously considered it." A second PEN American survey of 772 international writers living in 50 countries, conducted from August to October 2014 and later published in a report entitled "Global Chilling: The Impact of Mass Surveillance on International Writers" in January 2015, found 34% of writers living in "free countries" have "avoided writing or speaking on a particular topic, or have seriously considered it, due to fear of government surveillance," and another 42% have "curtailed or avoided activities on social media, or seriously considered it, due to fear of

[8] FDR GROUP & PEN AMERICAN CENTER, CHILLING EFFECTS: NSA SURVEILLANCE DRIVES U.S. WRITERS TO SELF-CENSOR 3–4 (2013), http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf; FDR GROUP & PEN AMERICAN CENTER, GLOBAL CHILLING: THE IMPACT OF MASS SURVEILLANCE ON INTERNATIONAL WRITERS (2015), http://www.pen.org/sites/default/files/globalchilling_2015.pdf.

government surveillance." Again, these findings are consistent with my conclusions here concerning chilling effects on Wikimedia users.

20. Other recent qualitative and quantitative studies also document how government surveillance has a chilling effect on various online and offline activities. Karin Wahl-Jorgenson et al.'s qualitative and quantitative study of how surveillance impacts U.K. journalists, published in a peer-reviewed paper in 2017, found "many" journalists interviewed "cited personal experience with surveillance" and how it has had a "chilling effect on reporting practices."[9] Lina Dencik and Jonathan Cable's qualitative study involving focus groups and interviews among journalists and activists in the United Kingdom, and published in a peer-reviewed journal in 2017, found evidence of surveillance chilling effects among participants "both for ordinary communication and for pursuing particular forms of social change or expressing dissent."[10] Paul Lashmar's study involving interviews with journalists after the Snowden revelations, published in a peer reviewed journal in 2017, found all participants believed the existence of mass government surveillance would "chill" and deter confidential sources from speaking with journalists.[11] Additionally, Margot Kaminski and Shane Witnov's 2015 law review article cites a range of other social science

[9] Karin Wahl-Jorgensen, Lucy K. Bennett, & Jonathan Cable, *Surveillance Normalization and Critique: News coverage and journalists' discourses around the Snowden revelations*, 5(3) DIGITAL JOURNALISM 386 (2017).

[10] Lina Dencik and Jonathan Cable, *The Advent of Surveillance Realism: Public Opinion and Activist Responses to the Snowden Leaks*, 11 INTERNATIONAL JOURNAL OF COMMUNICATION 763 (2017).

[11] Paul Lashmar, *No more sources? The impact of Snowden's revelations on journalists and their confidential sources*, 11(6) JOURNALISM PRACTICE 665 (2017).

research to support the assumption that surveillance has a chilling effect on speech and other behavior.[12]

21. Finally, my own survey-based study of over 1200 American Internet users, published in a peer-reviewed journal in 2017, found that awareness of possible government online surveillance has a chilling effect on a range of online activities, including 62% of participants being much less likely or somewhat less likely to "speak or write about certain topics online"; 78% indicating they would be "more careful" about what they "search for online"; and 60% being much less or somewhat less likely to share personally created content online, among other findings.[13] I also found that participants with greater awareness of news about the NSA were statistically more chilled by government surveillance. All of these studies, and their findings, support my conclusions here concerning chilling effects on Wikimedia users.

V. WIKIPEDIA STUDY—DESIGN, METHOD, AND RESULTS

22. As part of my doctoral research at Oxford, I designed an empirical study to test chilling effects theory, focusing on Internet user interaction with Wikipedia, one of the world's most viewed websites and an important source knowledge and information for people around the globe. The study examined Wikipedia article page view traffic before and after June 2013, to test the hypothesis that increased public awareness about NSA surveillance would lead to users being less likely to view Wikipedia articles on certain privacy-sensitive topics. This Part summarizes the study's design, methodology, and findings.

---

[12] *See* Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 480 (2015).

[13] Jonathon Penney, *Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study*, 6(2) INTERNET POLICY REVIEW (2017).

A. Design

23. My design emphasizes a quasi-experimental approach—commonly accepted in social science—to understanding the impact of NSA surveillance activity on user behavior—studying behavior both immediately following the June 2013 revelations, described as "level" changes, and the longer-term rates of viewership, described as "trend" changes. Combined, the decrease in level and trend constitute the full "chilling effect" of NSA surveillance.

24. To test my hypothesis, I used the most robust experimental design available given the available information and context around the NSA surveillance revelations. The "gold-standard" approach, randomized control trials, for definitive proof of a causal relationship between the NSA activity and viewership is not possible in this instance, as the revelations were widespread and impossible to assign randomly. Thus, I chose a robust quasi-experimental approach common in social science research—an interrupted time series (ITS) design with segmented regression analysis. ITS offers a powerful statistical means to analyze whether page views for privacy-concerning Wikipedia articles were impacted by public awareness about NSA surveillance programs after the June 2013 Snowden revelations.[14] In an ITS design, a series of observations on the same outcome, collected at equally spaced intervals over time, before and after an

[14] For discussion of interrupted time series research design, see DONALD T. CAMPBELL, JULIAN C. STANLEY & NATHANIEL L. GAGE, EXPERIMENTAL AND QUASI-EXPERIMENTAL DESIGNS FOR RESEARCH 37–43 (1966) (discussing the components of time series designs and their methodological advantages and limitations); A.K. Wagner et al., *Segmented Regression Analysis of an Interrupted Time Series in Medication Use Research*, 27 J. CLINICAL PHARMACY & THERAPEUTICS 299 (2002) (discussing advantages of using of segmented regression analysis along with ITS design); Monica Taljaard et al., *The use of segmented regression in analysing interrupted time series studies: an example in pre-hospital ambulance care*, 9 IMPLEMENTATION SCIENCE 1 (2014); Mylene Lagarde, *How to do (or not to do) … Assessing the impact of a policy change with routine longitudinal data*, 27:1 HEALTH POLICY AND PLANNING 76 (2012); Robert B. Penfold & Fang Zhang, *Use of Interrupted Time Series Analysis in Evaluating Health Care Quality Improvements*, 13:6 ACAD. PEDIATRICS S38 (2013) (discussing the advantages and limitations of employing time series analysis to understand and explore the impact of policy changes).

intervention, are used to test the immediate and longer term effect of the intervention.[15] A major strength of the design is its ability to distinguish the impact or effect of an intervention from the "secular" trend, that is, the trend or changes that would have occurred over time but for the intervention.[16]

25. In order to be a valid indicator of causal change, an ITS design requires primarily that the point of "intervention"—in this case public knowledge of NSA surveillance activities—be clear and fairly immediate. The prior research cited above on public awareness supports this date as an unambiguous intervention point to use when testing this hypothesis, and I further lay out evidence of public awareness below. I also conducted ITS segmented regression on "comparator" articles with the same intervention point to further test the ITS approach with reasonable "control" groups, insolating the impacts of the intervention. The effects of an ITS are estimated by comparing both level and trend in the pre- and post-intervention periods through the use of segmented regression. Here, the time period studied before and after the June 2013 revelations is long enough to control for overall trends (for example, seasonality or other long-term changes in page views) and to determine if the decline in page views was temporary or more permanent and damaging. The data after the intervention have a different level and trend than the pre-intervention series, indicating public awareness of NSA surveillance impacted users' Wikipedia use.

i. Intervention Selection

26. On June 6, 2013, stories in The Guardian and *The Washington Post* detailed previously undisclosed information and leaked classified documents about the surveillance practices of the

[15] Taljaard, *id.*; Lagarde, *id.*

[16] Taljaard, *id.*

United States and other Western governments.[17] The June 2013 revelations (also, "Snowden revelations") were followed by stories in June and subsequent months covering a vast array of government surveillance practices and operations.[18]

27. The revelations caused a "media and political storm," receiving widespread coverage both in traditional and new media outlets, and sparking a "heated international debate" in the United States, Europe, Russia, and beyond.[19]

28. Governments cited the "War on Terror" to defend the surveillance programs, and this justification was reflected in media coverage of the Snowden revelations.[20] The Snowden leaks and coverage, as media scholar Vian Bakir has noted, highlighted the previously limited public awareness about government surveillance activities while also augmenting that awareness.[21]

29. Indeed, in the United States, the widespread media coverage has led to greater awareness and concern among the general public about government surveillance activities and

---

[17] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 6, 2013), http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secretprogram/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497story.html; Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[18] *See* David Lyon, *Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique*, 1 BIG DATA & SOC'Y 1, 2 (2014) (discussion and analysis of subsequent news stories covering surveillance revelations).

[19] Vian Bakir, *Agenda Building, and Intelligence Agencies: A Systematic Review of the Field from the Discipline of Journalism, Media, and Communications*, 20 INT'L J. PRESS/POL. 131 (2015).

[20] *Id*. at 133; *see* Jie Qin, *Hero on Twitter, Traitor on News: How Social Media and Legacy News Frame Snowden*, 20 INT'L J. PRESS/POL.166 (2015) (finding that a predominant "framing" in traditional news media coverage of the Snowden surveillance disclosures focused on national security terrorism, along with international relations).

[21] *See* Bakir, *supra* note 19, at 133.

anti-terrorism efforts more generally. A Pew study in 2014 found that 87% of U.S. adults had heard something about "the government collecting information about telephone calls, e-mails, and other online communications" as part of "efforts to monitor terrorist activity" (with 43% hearing "a lot" and 44% hearing "a little"); another 80% agreed or strongly agreed that "Americans should be concerned" about government surveillance.[22] This increased awareness of online government surveillance presented a unique opportunity for chilling effects research. The surveillance revelations and widespread surrounding publicity constituted an "exogenous shock," or focal point, to study the effects of surveillance on Internet use behavior.

30. I examined view count data for privacy-sensitive Wikipedia articles before and after June 2013, to see if the greater awareness about potential NSA surveillance online may have "chilled" or deterred Internet users from viewing such privacy-sensitive content on Wikipedia. In other words, I tested the following hypothesis: due to chilling effects caused by increased awareness of NSA surveillance online, including Upstream surveillance, Internet users will be less likely to view Wikipedia articles on topics that raise privacy-related concerns.

ii. Data Selection

31. To select privacy-sensitive Wikipedia articles to track in the study, I matched 48 Wikipedia articles with a list of "terrorism" related keywords that the U.S. Department of Homeland Security (DHS) uses to track and monitor social media.[23] This DHS keyword list

[22] MARY MADDEN, PUBLIC PERCEPTIONS OF PRIVACY AND SECURITY IN THE POST-SNOWDEN ERA, PEW RES. INTERNET PROJECT 2–3 (Nov. 12, 2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf.

[23] The keyword list has been publicly available online since 2012, and was updated and re-posted by the DHS in 2013: U.S. DEP'T OF HOMELAND SEC., NATIONAL OPERATIONS CENTER MEDIA MONITORING CAPABILITY ANALYST'S DESKTOP BINDER (2011), https://epic.org/foia/epic-v-dhs-media-monitoring/Analyst-Desktop-Binder-REDACTED.pdf. This was later updated and posted online by the DHS. *See* U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE OFFICE OF

categorizes certain search terms or keywords in relation to a range of different issues such as "Health Concern," "Infrastructure Security," and "Terrorism." Forty-eight Wikipedia articles were included in the study that corresponded with DHS keywords listed as relating to "terrorism" ("Terrorism Wikipedia Article Group").[24] The Terrorism Wikipedia Article Group included articles on "dirty bomb," "suicide attack," "nuclear enrichment," and "eco-terrorism," among others.[25] Keywords relating to "terrorism" were used because the U.S. Government cited terrorism as a key justification for its online surveillance practices and media coverage largely framed the Snowden revelations around terrorism and national security.[26]

32. The DHS keyword list was used for pragmatic methodological reasons, that is, a non-random means to select groupings of Wikipedia articles. It was hypothesized that Wikipedia articles coinciding with these terrorism-related topic keywords may include the kind of information or content users may avoid accessing in light of potential government surveillance. To test that hypothesis, a survey of 415 independent Internet users was also conducted to provide additional evidence that Wikipedia articles associated with these "terrorism" keywords raised

---

OPERATIONS COORDINATION AND PLANNING (2013), https://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia_ops_NOC%20MMC%20Update_April2013.pdf.

[24] Locating Wikipedia articles coinciding with each keyword was done manually; there was a Wikipedia article that corresponded perfectly with the vast majority of keywords in the "terrorism" DHS keyword category. There were a few discrepancies, however: the Wikipedia article "environmental terrorism" was used for the keyword "environmental terrorist"; the keyword "target" was excluded as they were too many potentially corresponding Wikipedia articles; the Wikipedia article "political radicalism" was used for the DHS keyword "radicalism" because there were too many potentially corresponding articles; the keyword "enriched" was excluded as it was redundant with the included Wikipedia article "nuclear enrichment"; and there were also no Wikipedia articles corresponding with DHS keywords "weapons cache," "suspicious substance," "plot," and "homegrown." Wikipedia articles corresponding with the remaining 48 DHS "terrorism"-related keywords were all included in the study.

[25] *See infra* Appendix A, Table 11 ("48 Terrorism Article Group" list), Table 12 (privacy-sensitive score for each of 48 articles).

[26] *See supra* note 20.

privacy concerns for Internet users aware of government surveillance online. Respondents in the survey were recruited through Amazon's Mechanical Turk ("MTurk"), a platform researchers have used to carry out a range of empirical and social science research, including survey research.[27]

33. A total of 415 independent Internet users participated in the crowdsourcing project through MTurk, and they rated each of the 48 topics to which the Wikipedia articles in the data set corresponded. The survey questions were designed to explore the likelihood that the topics would raise privacy-related concerns for Internet users.[28] To minimize self-selection and response bias (a limitation difficult to avoid in non-random sampling), the brief questionnaires were described as merely an "Online Information Study" to potential MTurk participants. The results from the survey are set out in Table 10 and Table 12 of Appendix A.

iii. Data Collection

34. Having selected the 48 Terrorism Wikipedia Articles Group, the study aggregated Wikipedia article view count data on a monthly basis for these Wikipedia articles over a 32-month period, from the beginning of January 2012 to the end of August 2014. The study used data for English language article view counts from stats.grok.se, an online portal that provided access to non-mobile Wikipedia article view count data on a daily and monthly basis, and which was based

[27] Gabriele Paolacci & Jesse Chandler, *Inside the Turk: Understanding Mechanical Turk as a Participant Pool*, 23:3 CURRENT DIRECTIONS PSYCHOL. SCI. 184, 186 (2014), http://cdp.sagepub.com/content/23/3/184.abstract; Matthew J.C. Crump, John V. McDonnell & Todd M. Gureckis, *Evaluating Amazon's Mechanical Turk as a Tool for Experimental Behavioral Research*, 8:3 PLOS ONE e57410, e57410 (2013), http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0057410.

[28] Respondents were asked to indicate on a scale of 1 to 5 (1 being very unlikely and 5 being very likely): how likely they thought they would be in trouble if the U.S. government found out that they accessed information about the topic in question (Government Trouble Rating); how "privacy-sensitive" they viewed each topic as (in this case, 5 being highly sensitive and 1 not at all) (Privacy-Sensitive Rating); how likely they would be to delete the browser history on their computer after accessing information about the topic (Browser Delete Rating); and how likely they would avoid viewing or accessing information on the topic if they knew the Government was monitoring people's activities online (Avoidance Rating).

on a Wikimedia maintained page view dataset. The portal has been used in a range of peer-reviewed research.[29] These Wikipedia article views, or "page views," represent the number of times a Wikipedia article was "requested" from Wikimedia's servers (such as by a non-mobile web browser user clicking on a link to load the Wikipedia article).[30] The Terrorism Wikipedia Articles generated nearly 81 million total page views over the course of the 32-month study period.

B. Method of Analysis

35. A strength of an ITS design is that there are multiple measures before and after the intervention in the time series; such multiplicity controls for changes in level and trends in the data and increases the robustness of results.[31] Thus, my study used Wikipedia article view counts to create a time series over a 32-month period from January 2012 to August 2014 (n=32), with the June 2013 NSA surveillance revelations as the "intervention" that interrupts the time series, dividing it into two segments: before and after June 2013. The study also isolated the impact and lasting effect of the intervention by similarly analyzing the level and trend data for "comparator" Wikipedia articles groups.

---

[29] Research has included studies involving market trends, health information access, and social-political change, among others. *See, e.g.*, Michela Ferron & Paolo Massa, *WikiRevolutions: Wikipedia as a Lens for Studying the Real-Time Formation of Collective Memories of Revolutions*, 5 INT'L J. COMM. 1313 (2011) (examining Wikipedia as a "lens" through which to understand real-time social and political upheaval and change); Michaël R. Laurent & Tim J. Vickers, *Seeking Health Information Online: Does Wikipedia Matter?* 16:4 J. AM MED. INFORMATICS ASS'N 471 (2009) (using Wikipedia traffic data from stats.grok.se to study the relevance of Wikipedia to how people access to health information online); Helen Susannah Moat et al., *Quantifying Wikipedia Usage Patterns Before Stock Market Moves*, 3 SCI. REP. 1 (2013) (investigating Wikipedia article traffic and usage in relation to stock market changes).

[30] The raw Wikipedia article page view statistics track total views or loads of the Wikipedia articles or pages in question, not unique visitors. *See Pageview Statistics*, WIKIPEDIA.ORG, https://en.wikipedia.org/wiki/Wikipedia:Pageview_statistics.

[31] *See* CAMPBELL, STANLEY & GAGE, *supra* note 14, at 37; Lagarde, *supra* note 14; Penfold & Zhang, *supra* note 14, at S39; Wagner et al., *supra* note 14, at 308.

36. Two statistical approaches were used to analyze the interrupted time series. I first conducted a simple comparison of the mean number of views for all the Wikipedia articles in the dataset before and after June 2013. Second, I used a segmented regression analysis to estimate article view trends for the pre/post time segments. The results are reported and analyzed in what follows, with statistically significant findings tabulated and presented graphically.[32]

37. Autocorrelation is the tendency for observations taken over a period of time to be correlated or related to each other. It can be a potentially confounding factor for statistical results arrived at through an ITS design.[33] My study corrected for auto-correlation using the Prais-Winsten method for the second set of results described below—the 47 Wikipedia Terrorism Article Group—and one comparator group, the 34 infrastructure-related Article Group.[34] *See infra* Part C.ii-iii (results for these two sets of article groups).

---

[32] A statistically significant result is a result that is not attributed to random chance. Statistical hypothesis testing is used to determine whether the result of a data set is statistically significant. This test provides a probability value or *p*-value, which represents the probability that random chance could explain the result. Generally, a *p*-value of 0.05 or lower is considered to be statistically significant. It means there is a less than 5% chance that the results are explained by chance, and thus this low probability means we can reject to "null" hypothesis, which assumes that any effect or result is due to chance. A *p*-value of 0.01 or lower, which means there is a less than 1% chance that the results are explained by chance, is considered to be highly statistically significant. John Concato & John A Hartigan, *P values: from suggestion to superstition*, 64 JOURNAL OF INVESTIGATIVE MEDICINE 1166, 1166–67 (2016); Valen E. Johnson, *Revised standards for statistical evidence*, 110:48 PNAS 19313, 19313, 19316 (2013) (describing the "classical hypothesis tests", including "highly significant" p-value level at 0.01); David M. Lane, *Significance Testing*, in (David M Lane, ed.) ONLINE STATISTICS EDUCATION: AN INTERACTIVE MULTIMEDIA COURSE OF STUDY 376, 376–77 (2018), http://onlinestatbook.com/Online_Statistics_Education.pdf.

[33] The Durbin-Watson Test Statistic provides a diagnostic test for autocorrelation. *See* Lagarde, *supra* note 14 at 77, 79. A general rule of thumb is a Durbin-Watson Test result of 1.5 to 2 discloses no autocorrelation concern, while a result closer to 1 (or less) or 3 (or more) may suggest autocorrelation. *See* W. PAUL VOGT & R. BURKE JOHNSON, A DICTIONARY OF STATISTICS & METHODOLOGY: A NONTECHNICAL GUIDE FOR THE SOCIAL SCIENCES 118 (2011).

[34] The Durbin-Watson autocorrelation diagnostic test only showed autocorrelation concerns for these two Article Groups. The Prais-Winsten method is the recommended statistically method to control for auto-correlation. *See* Lagarde, *supra* note 14 at 77, 79.

C. Results

38. The results described below provide evidence of a chilling effect associated with the June 2013 public awareness about NSA surveillance programs.

i. First Set of Results: 48 Terrorism Wikipedia Article Group

39. The average monthly views for all 48 Wikipedia articles in the Terrorism Wikipedia Article Group combined show a noteworthy decrease in views after June 2013. Figure 1 illustrates this decline in page views pre- and post- June 2013, over the course of the 32-month period from January 2012 to August 2014.

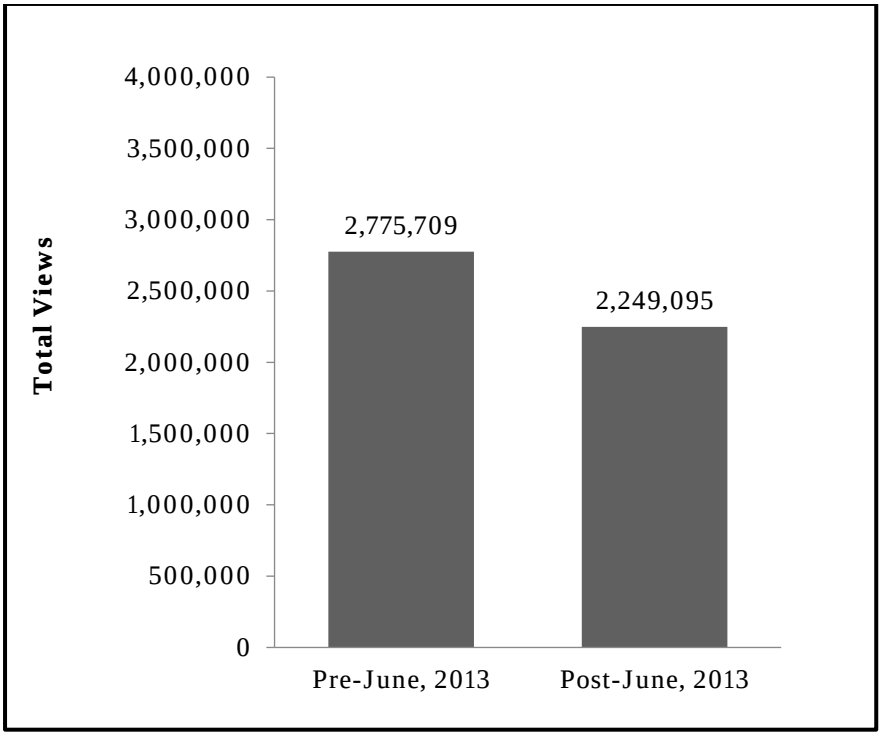


Figure 1. *Average Monthly View Counts, Pre- and Post- June 2013. The reduction after the June 2013 surveillance revelations is consistent with a chilling effect.*

40. The difference in mean monthly page views before and after June 2013 is notable—a reduction of 526,614 in the average monthly views for the articles, which represents approximately

a 19.5% drop in article view counts. This difference is statistically significant[35] and consistent with a chilling effect. To strengthen this inference, further analysis was done using segmented regression, a statistical method of analysis that controls for other variables.

41. The results based upon the more robust segmented regression statistical analysis are also consistent with the hypothesized chilling effects. The first set of results (*see* Table 1 of Appendix A) show that, based on the monthly article view trend existing before June 2013, there was a reduction of 995,085 article views in June 2013, which was a large, sudden, and statistically significant drop in the total view counts for the 48 Terrorism Wikipedia Article Group. The predicted article views for the month of June 2013 based on the pre-June monthly article view trends was 3,199,053, meaning the 995,085 reduction represents an immediate drop-off of 31%. The 31% drop in total view counts is consistent with an immediate and noteworthy chilling effect following the June 2013 revelations.

42. The chilling effect conclusion is further strengthened once the "Hamas" Wikipedia article was excluded from the 48 Terrorism Wikipedia Article Group. The Hamas Wikipedia article was a significant outlier,[36] with view counts skyrocketing in November 2012 and July 2014,

[35] "Cohen's *d*" is a test used to determine the "effect size" of a difference between two means, that is, whether the difference (as here) is substantial enough to be meaningful. It is calculated by dividing the means by the standard deviation. A result of 0.8 or more is considered a large effect. Here, the Cohen's *d* value was over 1. *See* David M. Lane, *The Difference Between Two Means*, in (David M Lane, ed.) ONLINE STATISTICS EDUCATION: AN INTERACTIVE MULTIMEDIA COURSE OF STUDY 349, 349 (2018), http://onlinestatbook.com/Online_Statistics_Education.pdf.

[36] Model diagnostics identified two influential outlier data points. The first outlier concerned view counts for the Wikipedia articles in the data set in November 2012 (Cooks D value = 0.1644942), and the other was for view counts in July 2014 (Cooks D value = 0.4121233). Examining more closely the view counts for the entire 48 Wikipedia articles in group, the Hamas article stood out: it had view counts of 928,533 for November 2012, and then 1,220,490 for July 2014, which are far beyond the mean number of view counts for the article across all months in the study (134,574 monthly views). If we exclude these two outlier months, the contrast between the view counts for the Hamas article during those two months and other months in the dataset is even starker, with the mean being 71,912. An assessment that these view counts were outliers is confirmed by the z-scores for those two data points (3.01 and 4.11, respectively).

which corresponded with Gaza conflicts between Hamas and the Israeli Defense Force during those months.[37] Once this single Wikipedia article was excluded, an even clearer picture emerged from the data.

ii. Second Set of Results: 47 Wikipedia Terrorism Article Group (Without Hamas Outlier)

43. Similar to the first set of results, this second set of results (set out in Table 2 of Appendix A) for the 47 Terrorism Wikipedia Article Group (excluding the Hamas article outlier) also showed an immediate and statistically significant decrease in view counts following increased public awareness about NSA surveillance in June 2013: an immediate drop of 693,617 total views. Using the predicted 3,034,721 article views for June 2013 based on the pre-June trend, this reduction represents an immediate drop-off of 23%. This similarly sharp and sudden decrease in view counts after June 2013 is consistent with a chilling effect.

44. Importantly, the second results also showed a statistically significant change in the overall trend in the month-to-month views of the 47 Terrorism Wikipedia Articles Group. Rather than increasing on a monthly basis, the page view trend after June 2013 is decreasing. Before June 2013, the data show an increase of 41,421 views per month. After June 2013, the data show a decrease of 67,513 in views per month. This change is important because it means that the public awareness about NSA surveillance programs is associated with a longer term decrease in views

[37] For a "timeline" of the conflict and the IDF operation against Hamas, see *TIMELINE: Israel Launches Operation Pillar of Defense Amid Gaza Escalation*, HAARETZ (Nov. 20, 2012), http://www.haaretz.com/news/diplomacy-defense/timeline-israel-launches-operation-pillar-of-defense-amid-gaza-escalation.premium-1.479284l; Amos Harel, *At the Crossroads of a Gaza Ground Operation*, HAARETZ (Jul. 12, 2014), http://www.haaretz.com/news/diplomacy-defense/.premium-1.604601. The notion that major conflicts, including the Gaza conflicts, draw "significantly higher levels" of activity on the social media platform Twitter is consistent with findings from previous research. *See* Thomas Zeitzoff, John Kelly & Gilad Lotan, *Using Social Media to Measure Foreign Policy Dynamics: An Empirical Analysis of the Iranian–Israel Confrontation (2012–13)*, 52 J. PEACE RES. 368, 372 (2015).

for the Wikipedia articles studied, consistent with a longer term chilling effect; Figure 3 illustrates this trend. Figure 2 below illustrates both the statistically significant drop off and shift in the overall trend in the view count data after June 2013.

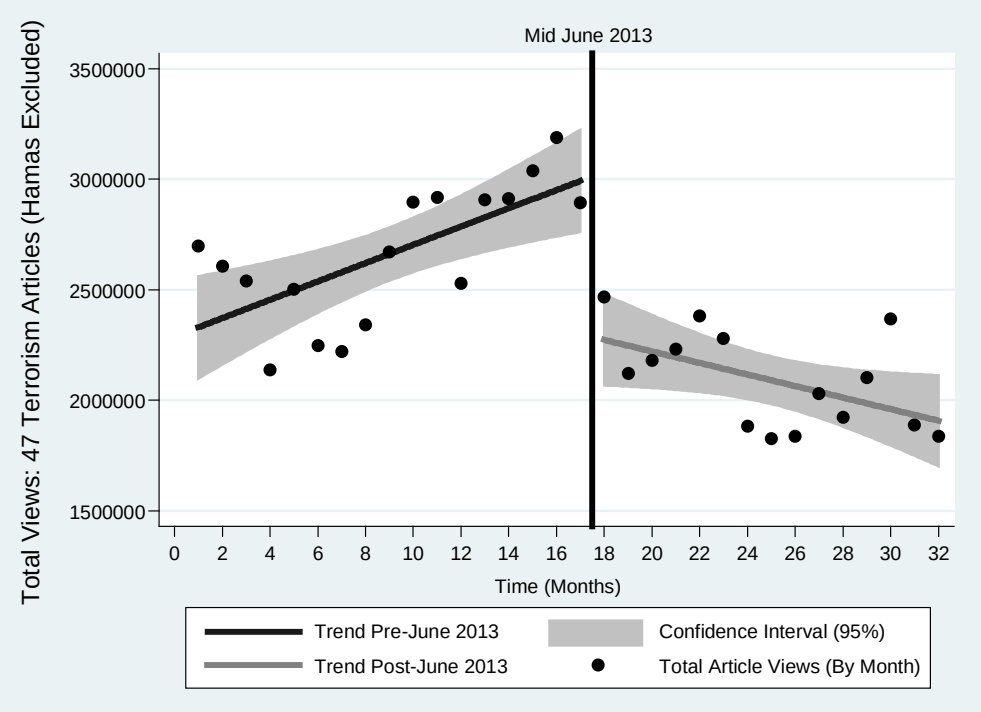


Figure 2. *Pre and Post June 2013 Article View Trends (Outliers Excluded). The sudden drop in views and trend shift—from increasing monthly views over time to decreasing after June 2013—is consistent with a significant and long-term chilling effect.*

45. The shifting trend of the data, which in this case is a sudden and immediate drop, is particularly consistent with a chilling effect arising from the public awareness about NSA surveillance after the June 2013 revelations. If the outlier view count data relating to the Hamas article is excluded, the decline in page views is slightly less substantial (e.g., 23% compared to the 31% drop-off if the Hamas data remains in the study) but in either case, a substantial and statistically significant decrease.

46. Moreover, there is a change in the overall trend in the data. Before June 2013, total views of the Wikipedia articles in the dataset slowly increase each month. After June 2013,

however, with the increased public awareness about NSA surveillance programs, there is a change in the "slope," or data trend. Without the outlier "Hamas" view counts in July 2014, the total views for the Terrorism Wikipedia Articles Group are on a downward path as seen in Figure 2. All of this is consistent with a chilling effect associated with the public awareness about NSA surveillance programs due to June 2013 revelations and reporting—both the reduction in view counts in June 2013 and the overall shift in the monthly article view trend thereafter.

47. The data findings in Table 2 and visualized in Figure 2 offer evidence demonstrating a long-term chilling effect due to the June 2013 surveillance revelations, which is not only associated with an immediate drop in views but also a long-term chill on accessing these Wikipedia articles, as users accessed information on these topics less and less frequently.

iii. Third Set of Results: 31 Most Privacy-Sensitive Wikipedia Terrorism Article Group

48. An additional analysis of the 31 most privacy-concerning Wikipedia articles in the 47 Terrorism Wikipedia Article Group (the articles associated with keywords receiving the highest sensitivity responses in the MTurk survey described in ¶ 33)[38] strengthens the chilling effects hypothesis. Using the 983,860 predicted article views for June 2013 (based on the pre-June monthly view trend), showed an even greater reduction in views in June 2013 of 26% (highly statistically significant at $p<0.01$ level) as well as a highly statistically significant reversal in the overall month to month view counts, due to a reduction of 41,554 monthly views after June 2013. These results, where more privacy-concerning Wikipedia articles lead to an even greater statistically significant view count reduction in June 2013, as well as a likewise reversal in the overall article views on a monthly basis after June 2013, is consistent with a chilling effect

[38] This set includes the 31 terrorism-related articles, among the full-set of 48, that had a combined average privacy rating score above 2 from the MTurk survey—the median score for the set of 48. *See infra* Appendix A, Table 13 ("31 Article Group" list including combined privacy-sensitive score).

hypothesis. Correcting for auto-correlation using the Prais-Winsten method for the 47 Terrorism Wikipedia Article Group did not change these key findings.

49. Further strengthening this chilling effects hypothesis, overall Wikipedia article view traffic trends do not explain these results. Identical analysis of view counts for the English Wikipedia home page (non-mobile platforms data) for the same 32-month period can be found at Table 3 of Appendix. There are clear differences. First, while there is a reduction in views for the English Wikipedia homepage in June 2013, the reduction is significantly less (16% if one considered predicted views for June 2013 based on previous trends). So, even assuming a full 16 percentage points in the total 23% drop off for the 47 terrorism-related Wikipedia articles[39] simply reflects overall English Wikipedia trends, that still leaves 7% of the reduction in article views in June 2013. Similarly, using the 31 most privacy-concerning terrorism-related Wikipedia articles, which as noted above had a 26% reduction in June 2013,[40] would leave a 10% drop unaccounted for by background trends. This is more than twice the noteworthy and statistically significant 4% reduction in Google privacy-sensitive searches that Marthews and Tucker found after June 2013.

50. Moreover, while there is a statistically significant change in monthly article views after June 2013 for the English Wikipedia Homepage, there are again significant differences. The monthly rate of change before June 2013 for the homepage was less than 1 percent of views per month (0.97%) and after June 2013, views reduced on a monthly basis by 0.22%. By stark contrast, the results for the 31 most privacy-concerning Wikipedia Terrorism Articles Group showed that before June 2013, there was a statistically significant monthly increase in views that amounted to a 6% overall increase in article views per month, and after June 2013, monthly views decreased

[39] *See supra* ¶ 43.

[40] *See supra* ¶ 48.

by 2% a month. In other words, the 31 most privacy-concerning article views for these articles were increasing at six times the rate of the English Wikipedia homepage on a monthly basis, and after June 2013 were decreasing monthly at ten times the rate of the English Wikipedia homepage. These differences all suggest that these findings for the 47 Terrorism Wikipedia Articles Group and the 31 most privacy-concerning Terrorism Wikipedia Articles Group reflect more than mere background Wikipedia trends.[41]

51. A further analysis of the 31 most privacy-concerning Terrorism Articles Group, which includes English Wikipedia Homepage views (non-mobile platforms data) as a control (see Table 8), provides even more support. Using the 1,012,950 predicted article views for June 2013, these results also showed a greater reduction in views in June 2013 of 31% (highly statistically significant at $p<0.01$ level), as well as a highly statistically significant reversal in the overall month-to-month view counts, due to a reduction of 46,226 monthly views after June 2013. An identical analysis of the 47 Terrorism Articles Group, also with English Wikipedia Homepage views as a control (see Table 9), yielded a 20% highly statistically significant reduction in views in June 2013 and a highly statistically reversal in overall month-to-month view, due to a reduction of 60,504 monthly views after June 2013. There was also no correlation found between either the 31 or 47 Terrorism Article Groups and the English Wikipedia Homepage views. These findings are consistent with a chilling effects hypothesis.

iv. Comparator Wikipedia Article Groups

52. The conclusions of this statistical analysis are further strengthened by analyses carried out on three different "comparator" groups of Wikipedia articles. Using the same statistical methods described above, analyses of the comparator groups showed neither a statistically

[41] Marthews & Tucker, *supra* note 4, at 3.

significant reduction in article views in June 2013, nor a shift in the overall trend in article views after that month. These comparator Wikipedia article groups included a group of 25 security-related Wikipedia articles;[42] 34 infrastructure-related Wikipedia articles;[43] and a group of the 26 most popular Wikipedia articles in 2012, 2013, and 2014.[44]

53. As Figure 3 illustrates, unlike the 47 Terrorism Wikipedia Article Group, results from an identical analysis for the group of 25 domestic "security"-related Wikipedia articles showed no statistically significant reduction in article views in June 2013 and no statistically significant change in the trend in the data.

[42] The methodology for selecting Wikipedia articles for the security comparator group was the same as that used for the original 48 Wikipedia Terrorism articles. Wikipedia articles corresponding with keywords set out in the DHS keyword list for domestic security ("DHS & Other Agencies" keyword category) were included. Locating Wikipedia articles coinciding with each keyword was again done manually, and similarly, there was a Wikipedia article that corresponded perfectly with the vast majority of keywords in the "DHS & Other Agencies" keyword category. The 25 Wikipedia articles are included in Appendix A at Table 14.

[43] The methodology for selecting Wikipedia articles for the infrastructure group was the same as for the terrorism and domestic security Wikipedia article groups. Here, Wikipedia articles were selected that corresponded to DHS keywords for the "Infrastructure Security" keyword category. Again, locating articles was straightforward, as there was a Wikipedia article that corresponded naturally with the vast majority of keywords in the "Infrastructure Security" keyword category. All 34 Wikipedia articles are included in Appendix A at Table 15.

[44] The top 10 most popular English Wikipedia articles (in terms of article views) for each of years 2012, 2013, and 2014 (the years included in the 32-month study period) were included in the "popular" Wikipedia article comparator group. This was determined by consulting the Wikimedia Tool Lab's "Wikitrend" reports (https://tools.wmflabs.org/wikitrends), resulting in a set of 26 Wikipedia articles comparator group, including articles like "Google," "Facebook," "Breaking Bad," "Game of Thrones," and "World War II." Certain Wikipedia articles like "Facebook" and "Google" were in the top ten most popular articles for more than one year, hence 26 articles instead of 30. The 26 popular articles group is listed in Appendix A at Table 16.

Figure 3. *The highly statistically significant (at the $p<0.01$ level) substantial view count reduction in June 2013 as well as the shift to fewer monthly article views after June 2013 for the terrorism articles is consistent with a chilling effect. There are no statistically significant findings for the comparator article groups.*

Wikipedia Article Group	Monthly trend pre-June 2013	Change in view count in June 2013	Change in monthly trend after June 2013	Model Fit
47 Terrorism Articles	**41,420.51**** ***p*=0.00**	**−693,616.9**** ***p*=0.00**	**−67,513.1**** ***p*=0.00**	**Yes** ***F*=0.00**
25 Security Articles	11,135.0 *p*=0.187	−24,638.34 *p*=0.84	−20,465.87 *p*=0.12	No *F*=0.45
34 Infrastructure Articles	**−11,079**** ***p*=0.00**	−12,721.0 *p*=0.77	2,431.84 *p*=0.61	**Yes** ***F*=0.00**
26 Popular Articles	−48,458 *p*=0.798	−1,716,643 *p*=0.53	177,324.7 *p*=0.551	No *F*=0.79

Statistically significant findings in bold (*p<0.05, **p<0.01).

54. In fact, the overall model fit for this analysis was not significant, meaning the public awareness about NSA surveillance programs in June 2013 revelations has no value for predicting article views and view trends for these 25 domestic security related articles.[45]

55. The 34 "infrastructure" Wikipedia article comparator group results also showed no statistically significant reduction in article view counts after the June 2013 revelations, nor any statistically significant change in the overall month-to-month trend in the view count data after that month. Correcting for autocorrelation in these results does not change these key observations.

56. Finally, the results for an identical analysis on the 26 "popular" Wikipedia article comparator group likewise showed no statistically significant reduction in views or any monthly

[45] When the F-test or F-value for a regression analysis result is not significant (greater than 0.05) then the analysis (and results) are not reliable and have no predictive value. *See* Karen Grace-Martin, *Assessing the Fit of Regression Models*, THE ANALYSIS FACTOR: MAKING STATISTICS MAKE SENSE (Online), https://www.theanalysisfactor.com/assessing-the-fit-of-regression-models/; MARKO SARSTADT AND ERIK MOOI, A CONCISE GUIDE TO MARKET RESEARCH: THE PROCESS, DATA, AND METHODS USING IBM SPSS STATISTICS 212 (2014).

change in view count trends in relation to June 2013. Like the security comparator groups, the model fit for this analysis was not significant.

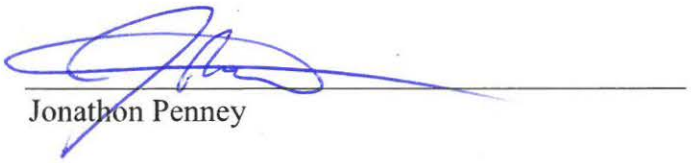
57. These results are all consistent with a chilling effects hypothesis. Unlike the privacy-concerning 47 Terrorism Wikipedia Article Group, the comparator Wikipedia article groups showed no comparable page view reductions in June 2013, nor a change in view count data trends after June 2013. These comparator results strengthen the conclusion that the statistically significant shift in article view counts post-June 2013 for the privacy-concerning Wikipedia articles is attributable to NSA-related chilling effects, and not to other background or confounding variables.

VI. CONCLUSION

58. In sum, I conclude that the highly statistically significant and substantial reduction in view counts in June 2013, as well as the highly statistically significant trend reversal in the monthly article views after June 2013, for both the 47 Terrorism Wikipedia Articles Group and the 31 most privacy-concerning Terrorism Wikipedia Articles Group, offers compelling evidence that increased public awareness about NSA surveillance programs in June 2013 had a chilling effect on Wikipedia users.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Executed on December 18, 2018 in Halifax, Canada.



Jonathon Penney

APPENDIX A

Table 1: First Results, 48 Terrorism-related Articles Study Group

(No autocorrelation concerns with Durbin-Watson Test of 1.50)

Independent Variable	Coefficients	Standard Error	*P*-value
Coefficient (β_0)	**23522364****	171743.1	0.000
Expected Total Views at Beginning of Study			
Pre June 2013 trend in data (β_1)	**47038.28****	16760.41	0.009
Change in Views (Monthly) Before 6/2013			
Change in level (β_2)	**−995085.2***	241987.6	0.000
Change in Views Immediately After 6/2013			
Change in slope (β_3)	−35517.69	26272.41	0.187
Change in Views (Monthly) After 6/2013			

*$p<0.05$, **$p<0.01$

Table 2: Second Results, 47 Terrorism-related Articles (Hamas Excluded)

Durbin-Watson Test Result (1.33)
Results correcting auto-correlation (Prais–Winsten method) in parenthesis

Independent Variable	Coefficients	Standard Error	*P*-value
Coefficient (β_0)	**2289153**** **(2349041.0)**	109751.5 (144474.7)	0.000 (0.000)
Expected Total Views at Beginning of Study			
Pre June 2013 trend in data (β_1)	**41420.51**** **(34813.9)***	10710.65 (13824.52)	0.001 (0.02)
Change in Views (Monthly) Before 6/2013			
Change in level (β_2)	**−693616.9 **** **(−594574.2)****	154640.9 (186174.7)	0.000 (0.00)
Change in Views Immediately After 6/2013			
Change in slope (β_3)	**−67513.1**** **(−65683)****	16789.25 (22514.01)	0.000 (0.00)
Change in Views (Monthly) After 6/2013			

*$p<0.05$, **$p<0.01$

Table 3: Global English Wikipedia Article Views, Non-Mobile (Millions)

(No autocorrelation concerns with Durbin-Watson Test of 1.89)

Independent Variable	Coefficients	Standard Error	*P*-value
Coefficient (β_0)	**7385.11****	204.48	0.000
Expected Total Views at Beginning of Study			
Pre June 2013 trend in data (β_1)	**70.57****	19.95	0.000
Change in Views (Monthly) Before 6/2013			
Change in level (β_2)	**−1397.96****	288.11	0.007
Change in Views Immediately After 6/2013			
Change in slope (β_3)	**−90.97****	31.28	0.000
Change in Views (Monthly) After 6/2013			

**p*<0.05, ***p*<0.01

Table 4: Full 25 Domestic Security-related Wikipedia Articles Comparator Group

Note: This model's fit was not significant (Prob > F = 0.447)

Independent Variable	Coefficients	Standard Error	*P*-value
Coefficient (β_0)	**708187.3****	84366.66	0.00
Expected Total Views at Beginning of Study			
Pre June 2013 trend in data (β_1)	11135.07	8233.34	0.187
Change in Views (Monthly) Before 6/2013			
Change in level (β_2)	−24638.34	118873.4	0.837
Change in Views Immediately After 6/2013			
Change in slope (β_3)	− 20465.87	12905.99	0.124
Change in Views (Monthly) After 6/2013			

**p*<0.05, ***p*<0.01

Table 5: 34 Infrastructure Security-related Articles Comparator Group

Durbin-Watson Test Result (1.09)
Results correcting auto-correlation (Prais–Winsten method) in parenthesis

Independent Variable	Coefficients	Standard Error	*P*-value
Coefficient (β_0)	**771772.3****	30948.71	0.000
	(785975.7)**	(42559.45)	(0.000)
Expected Total Views at Beginning of Study			
Pre June 2013 trend in data (β_1)	**−11079.82****	3020.28	0.001
	(−11847.06)**	(4040.79)	(0.007)
Change in Views (Monthly) Before 6/2013			
Change in level (β_2)	−12721.07	43607.01	0.773
	(−20678.15)	(52816.07)	(0.698)
Change in Views Immediately After 6/2013			
Change in slope (β_3)	2431.84	4734.38	0.612
	(3464.15)	(6663.93)	(0.607)
Change in Views (Monthly) After 6/2013			

**p*<0.05, ***p*<0.01

Table 6: 26 Most Popular Wikipedia Articles (2012/2013/2014) Comparator Group

Note: This model's fit was not significant (Prob > F = 0.7938)

Independent Variable	Coefficients	Standard Error	*P*-value
Coefficient (β_0)	**2.58×10^7****	1920624	0.000
Expected Total Views at Beginning of Study			
Pre June 2013 trend in data (β_1)	−48458.14	187433.7	0.798
Change in Views (Monthly) Before 6/2013			
Change in level (β_2)	−1716643	2706177	0.531
Change in Views Immediately After 6/2013			
Change in slope (β_3)	177324.7	293807.6	0.551
Change in Views (Monthly) After 6/2013			

**p*<0.05, ***p*<0.01

Table 7: 31 Terrorism-related Wikipedia Articles Study Group

No autocorrelation concerns with Durbin-Watson Test of 1.52

Independent Variable	Coefficients	Standard Error	*P*-value
Coefficient (β_0)	**471146.3****	45966.52	0.000
Expected Total Views at Beginning of Study			
Pre June 2013 trend in data (β_1)	**28484.1****	4485.87	0.000
Change in Views (Monthly) Before 6/2013			
Change in level (β_2)	**−253556.5****	64767.24	0.000
Change in Views Immediately After 6/2013			
Change in slope (β_3)	**−41554.21****	7031.73	0.000
Change in Views (Monthly) After 6/2013			

*$p<0.05$, **$p<0.01$

Table 8: 31 Terrorism-related Wikipedia Articles Study Group (with Control)

Results Controlling For English Wikipedia Homepage Views (Raw, Non-Mobile)
No autocorrelation concerns with Durbin-Watson Test of 1.62

Independent Variable	Coefficients	Standard Error	*P*-value
Coefficient (β_0)	**850386.4***	314365.4	0.01
Expected Total Views at Beginning of Study			
Pre June 2013 trend in data (β_1)	**32108.35****	5349.31	0.000
Change in Views (Monthly) Before 6/2013			
Change in level (β_2)	**− 325345****	87120.19	0.000
Change in Views Immediately After 6/2013			
Change in slope (β_3)	**−46226.01 ****	7955.04	0.000
Change in Views (Monthly) After 6/2013			
Global English Wikipedia Views Control	−51.35	42.11	0.233
Correlation with English Wikipedia Homepage Views (Non-mobile; in millions)			

*$p<0.05$, **$p<0.01$

Table 9: 47 Terrorism-related Wikipedia Articles Study Group (with Control)

Results Controlling For English Wikipedia Homepage Views (Raw, Non-Mobile)
Durbin-Watson Test Result (1.29)
Results correcting auto-correlation (Prais–Winsten method) in parenthesis

Independent Variable	Coefficients	Standard Error	*P*-value
Coefficient (β_0)	**1720195 ***	762994.1	0.03
	(1657787*)	(715964.1)	(0.03)
Expected Total Views at Beginning of Study			
Pre June 2013 trend in data (β_1)	**35983.25 ***	12983.28	0.01
	(29381.58)	(14928.98)	0.05
Change in Views (Monthly) Before 6/2013			
Change in level (β_2)	**−585915.8***	211448.8	0.01
	(−490610*)	(212517.7)	0.03
Change in Views Immediately After 6/2013			
Change in slope (β_3)	**− 60504.2****	19307.63	0.00
	(−56997.38*)	(24479.42)	0.03
Change in Views (Monthly) After 6/2013			
Global English Wikipedia Views Control	77.04	102.22	0.46
	(92.61)	(93.44)	(0.33)
Correlation with English Wikipedia Homepage Views (Non-mobile; in millions)			

*$p<0.05$, **$p<0.01$

Table 10: Independent Rating Results of 415 Internet Users

Rating Type	Mean Rating
Government Trouble Rating	1.95
Privacy-Sensitive Rating	2.01
Browser History Delete Rating	2.00
Avoidance Rating	2.62

Table 11: 48 Terrorism Article Group List

Topic Keywords	Wikipedia Articles
Al Qaeda	https://en.wikipedia.org/wiki/Al-Qaeda
terrorism	https://en.wikipedia.org/wiki/terrorism
terror	https://en.wikipedia.org/wiki/terror
attack	https://en.wikipedia.org/wiki/attack
Iraq	https://en.wikipedia.org/wiki/iraq
Afghanistan	https://en.wikipedia.org/wiki/afghanistan
Iran	https://en.wikipedia.org/wiki/iran
Pakistan	https://en.wikipedia.org/wiki/pakistan
agro	https://en.wikipedia.org/wiki/agro
Environmental terrorism	https://en.wikipedia.org/wiki/Environmental_terrorism
Eco terrorism	https://en.wikipedia.org/wiki/Eco-terrorism
Conventional weapon	https://en.wikipedia.org/wiki/Conventional_weapon
Weapons grade	https://en.wikipedia.org/wiki/Weapons-grade
dirty bomb	https://en.wikipedia.org/wiki/Dirty_bomb
Nuclear Enrichment	https://en.wikipedia.org/wiki/Nuclear_enrichment
Nuclear	https://en.wikipedia.org/wiki/nuclear
Chemical weapon	https://en.wikipedia.org/wiki/Chemical_weapon
Biological weapon	https://en.wikipedia.org/wiki/Biological_weapon
Ammonium nitrate	https://en.wikipedia.org/wiki/Ammonium_nitrate
Improvised explosive device	https://en.wikipedia.org/wiki/Improvised_explosive_device
Abu Sayyaf	https://en.wikipedia.org/wiki/Abu_Sayyaf
Hamas	https://en.wikipedia.org/wiki/hamas
FARC	https://en.wikipedia.org/wiki/FARC
Irish Republican Army	https://en.wikipedia.org/wiki/Irish_Republican_Army
Euskadi ta Askatasuna	https://en.wikipedia.org/w/Euskadi_ta_Askatasuna
Hezbollah	https://en.wikipedia.org/wiki/hezbollah
Tamil Tigers	https://en.wikipedia.org/wiki/Tamil_Tigers
PLO	https://en.wikipedia.org/wiki/Palestine_Liberation_Organization
Palestine Liberation Front	https://en.wikipedia.org/wiki/Palestine_Liberation_Front
Car bomb	https://en.wikipedia.org/wiki/Car_bomb
jihad	https://en.wikipedia.org/wiki/jihad
Taliban	https://en.wikipedia.org/wiki/taliban
Suicide bomber	https://en.wikipedia.org/wiki/Suicide_bomber
Suicide attack	https://en.wikipedia.org/wiki/Suicide_attack
AL Qaeda in the Arabian Peninsula	https://en.wikipedia.org/wiki/Al-Qaeda_in_the_Arabian_Peninsula
Al Qaeda in the Islamic Maghreb	https://en.wikipedia.org/wiki/Al-Qaeda_in_the_Islamic_Maghreb
Tehrik-i-Taliban Pakistan	https://en.wikipedia.org/wiki/Tehrik-i-Taliban_Pakistan
Yemen	https://en.wikipedia.org/wiki/yemen
Pirates	https://en.wikipedia.org/wiki/pirates
Extremism	https://en.wikipedia.org/wiki/extremism

Somalia	https://en.wikipedia.org/wiki/somalia
Nigeria	https://en.wikipedia.org/wiki/nigeria
Political radicalism	https://en.wikipedia.org/wiki/Political_radicalism
Al-Shabaab	https://en.wikipedia.org/wiki/Al-Shabaab
nationalism	https://en.wikipedia.org/wiki/nationalism
Recruitment	https://en.wikipedia.org/wiki/recruitment
Fundamentalism	https://en.wikipedia.org/wiki/fundamentalism
Islamist	https://en.wikipedia.org/wiki/islamist

Table 12: 48 Terrorism Article Group List with Privacy Survey Scores

Topic Keywords	Government Trouble	Browser Delete	Privacy Sensitive	Avoidance
Al Qaeda	2.20	2.11	2.21	2.84
terrorism	2.19	2.05	2.16	2.79
terror	1.98	1.96	2.01	2.64
attack	1.92	1.91	1.92	2.56
Iraq	1.60	1.74	1.76	2.25
Afghanistan	1.61	1.71	1.75	2.23
Iran	1.62	1.73	1.78	2.25
Pakistan	1.59	1.71	1.75	2.22
agro	1.51	1.80	1.76	2.29
Environmental terrorism	2.20	2.20	2.24	2.92
Eco terrorism	2.22	2.20	2.22	2.92
Conventional weapon	2.03	2.16	2.07	2.81
Weapons grade	2.18	2.22	2.17	2.99
dirty bomb	2.72	2.55	2.50	3.45
Nuclear Enrichment	2.22	2.21	2.21	2.92
Nuclear	1.84	1.97	1.91	2.55
Chemical weapon	2.43	2.36	2.39	3.16
Biological weapon	2.44	2.39	2.39	3.18
Ammonium nitrate	2.49	2.44	2.26	3.24
Improvised explosive device	2.82	2.64	2.53	3.46
Abu Sayyaf	2.02	1.96	1.99	2.57
Hamas	1.90	1.93	1.97	2.49
FARC	1.83	1.88	1.90	2.46
Irish Republican Army	1.62	1.77	1.83	2.24
Euskadi ta Askatasuna	1.86	1.88	1.88	2.43
Hezbollah	1.86	1.90	1.96	2.46
Tamil Tigers	1.76	1.86	1.87	2.39
PLO	1.77	1.87	1.91	2.42
Palestine Liberation Front	1.81	1.89	1.95	2.47
Car bomb	2.72	2.61	2.50	3.40
jihad	2.15	2.19	2.17	2.89
Taliban	2.06	2.03	2.10	2.70
Suicide bomber	2.25	2.31	2.24	2.97
Suicide attack	2.30	2.36	2.29	3.04
AL Qaeda in the Arabian Peninsula	2.01	1.98	2.06	2.63
Al Qaeda in the Islamic Maghreb	2.05	1.98	2.06	2.60
Tehrik-i-Taliban Pakistan	1.96	1.96	1.97	2.59
Yemen	1.60	1.72	1.74	2.18
Pirates	1.44	1.67	1.67	2.10
Extremism	1.64	1.90	1.86	2.40

Somalia	1.50	1.68	1.67	2.12
Nigeria	1.48	1.66	1.64	2.07
Political radicalism	1.75	1.91	1.97	2.48
Al-Shabaab	1.84	1.89	1.89	2.48
nationalism	1.48	1.71	1.73	2.20
Recruitment	1.74	1.90	1.87	2.54
Fundamentalism	1.60	1.79	1.80	2.32
Islamist	1.79	1.89	1.93	2.45
MEAN	**1.95**	**2.00**	**2.01**	**2.62**

Table 13: 31 Most Privacy-Concerning Terrorism Article Group (survey privacy-rating above 2)

Topic Keywords	Wikipedia Articles	Combined Privacy Rating
Al Qaeda	http://en.wikipedia.org/wiki/Al-Qaeda	2.34
terrorism	http://en.wikipedia.org/wiki/terrorism	2.30
terror	http://en.wikipedia.org/wiki/terror	2.15
Environmental terrorism	http://en.wikipedia.org/wiki/Environmental_terrorism	2.39
Eco terrorism	http://en.wikipedia.org/wiki/Eco-terrorism	2.39
Conventional weapon	http://en.wikipedia.org/wiki/Conventional_weapon	2.27
Weapons grade	http://en.wikipedia.org/wiki/Weapons-grade	2.39
dirty bomb	http://en.wikipedia.org/wiki/Dirty_bomb	2.81
Nuclear Enrichment	http://en.wikipedia.org/wiki/Nuclear_enrichment	2.39
Nuclear	http://en.wikipedia.org/wiki/nuclear	2.07
Chemical weapon	http://en.wikipedia.org/wiki/Chemical_weapon	2.59
Biological weapon	http://en.wikipedia.org/wiki/Biological_weapon	2.60
Ammonium nitrate	https://en.wikipedia.org/wiki/Ammonium_nitrate	2.61
Improvised explosive device	http://en.wikipedia.org/wiki/Improvised_explosive_device	2.86
Abu Sayyaf	http://en.wikipedia.org/wiki/Abu_Sayyaf	2.14
FARC	http://en.wikipedia.org/wiki/FARC	2.02
Euskadi ta Askatasuna	http://en.wikipedia.org/w/Euskadi_ta_Askatasuna	2.01
Hezbollah	http://en.wikipedia.org/wiki/hezbollah	2.05
Palestine Liberation Front	http://en.wikipedia.org/wiki/Palestine_Liberation_Front	2.03
Car bomb	http://en.wikipedia.org/wiki/Car_bomb	2.81
jihad	http://en.wikipedia.org/wiki/jihad	2.35
Taliban	http://en.wikipedia.org/wiki/taliban	2.22
Suicide bomber	http://en.wikipedia.org/wiki/Suicide_bomber	2.44
Suicide attack	http://en.wikipedia.org/wiki/Suicide_attack	2.50
AL Qaeda in the Arabian Peninsula	http://en.wikipedia.org/wiki/Al-Qaeda_in_the_Arabian_Peninsula	2.17
Al Qaeda in the Islamic Maghreb	http://en.wikipedia.org/wiki/Al-Qaeda_in_the_Islamic_Maghreb	2.17
Tehrik-i-Taliban Pakistan	http://en.wikipedia.org/wiki/Tehrik-i-Taliban_Pakistan	2.12
Political radicalism	http://en.wikipedia.org/wiki/Political_radicalism	2.03
Al-Shabaab	http://en.wikipedia.org/wiki/Al-Shabaab	2.03
Recruitment	http://en.wikipedia.org/wiki/recruitment	2.01
Islamist	http://en.wikipedia.org/wiki/islamist	2.02

Table 14: 25 Domestic Security Article List

Topic Keywords	Wikipedia Articles
Department of Homeland Security	https://en.wikipedia.org/wiki/United_States_Department_of_Homeland_Security
Federal Emergency Management Agency	https://en.wikipedia.org/wiki/Federal_Emergency_Management_Agency
Coast Guard	https://en.wikipedia.org/wiki/Coast_guard
Customs and Border Protection	https://en.wikipedia.org/wiki/Customs_and_Border_Protection
Border patrol	https://en.wikipedia.org/wiki/Border_Patrol
Secret Service	https://en.wikipedia.org/wiki/Secret_Service
Bureau of Land Management	https://en.wikipedia.org/wiki/Bureau_of_Land_Management
Homeland defense	https://en.wikipedia.org/wiki/Homeland_defense
Agent / Espionage	https://en.wikipedia.org/wiki/Espionage
Task Force 88	https://en.wikipedia.org/wiki/Task_Force_88_(anti-terrorist_unit)
Central Intelligence Agency	https://en.wikipedia.org/wiki/Central_Intelligence_Agency
Fusion center	https://en.wikipedia.org/wiki/Fusion_center
DEA	https://en.wikipedia.org/wiki/DEA
Secure Border Initiative	https://en.wikipedia.org/wiki/Secure_Border_Initiative
Federal Bureau of Investigation	https://en.wikipedia.org/wiki/Federal_Bureau_of_Investigation
Alcohol and Tobacco Tax and Trade Bureau	https://en.wikipedia.org/wiki/Alcohol_and_Tobacco_Tax_and_Trade_Bureau
U.S. Citizenship and Immigration Services	https://en.wikipedia.org/wiki/United_States_Citizenship_and_Immigration_Services
Federal Air Marshal Service	https://en.wikipedia.org/wiki/Federal_Air_Marshal_Service
Transportation Security Administration	https://en.wikipedia.org/wiki/Transportation_Security_Administration
Air Marshal	https://en.wikipedia.org/wiki/Air_marshal
Federal Aviation Administration	https://en.wikipedia.org/wiki/Federal_Aviation_Administration
National Guard	https://en.wikipedia.org/wiki/National_Guard
Disaster Relief / Emergency Management	https://en.wikipedia.org/wiki/Emergency_management
U.S. Immigration and Customs Enforcement	https://en.wikipedia.org/wiki/U.S._Immigration_and_Customs_Enforcement
United Nations	https://en.wikipedia.org/wiki/United_Nations

Table 15: 34 Infrastructure Article List

Topic Keywords	Wikipedia Articles
Information security	https://en.wikipedia.org/wiki/Infrastructure_security
Airport	https://en.wikipedia.org/wiki/Airport
Airplane	https://en.wikipedia.org/wiki/Airplane
Chemical burn	https://en.wikipedia.org/wiki/Chemical_burn
CIKR	https://en.wikipedia.org/wiki/CIKR
AMTRAK	https://en.wikipedia.org/wiki/Amtrak
Collapse	https://en.wikipedia.org/wiki/Collapse
Information infrastructure	https://en.wikipedia.org/wiki/Information_infrastructure
Telecommunications network	https://en.wikipedia.org/wiki/Telecommunications_network
Telecommunication	https://en.wikipedia.org/wiki/Telecommunication
Critical infrastructure	https://en.wikipedia.org/wiki/Critical_Infrastructure
National Information Infrastructure	https://en.wikipedia.org/wiki/National_Information_Infrastructure
Metro	https://en.wikipedia.org/wiki/Metro_station
WMATA	https://en.wikipedia.org/wiki/Washington_Metropolitan_Area_Transit_Authority
Subway	https://en.wikipedia.org/wiki/Subway
BART	https://en.wikipedia.org/wiki/Bay_Area_Rapid_Transit
MARTA	https://en.wikipedia.org/wiki/Metropolitan_Atlanta_Rapid_Transit_Authority
Port authority	https://en.wikipedia.org/wiki/Port_authority
NBIC	https://en.wikipedia.org/wiki/NBIC
Power grid	https://en.wikipedia.org/wiki/Electrical_grid
Power	https://en.wikipedia.org/wiki/Power
Smart	https://en.wikipedia.org/wiki/Smart
Full body scanner	https://en.wikipedia.org/wiki/Full_body_scanner
Electric power	https://en.wikipedia.org/wiki/Electric_power
Failure	https://en.wikipedia.org/wiki/Failure
Power outage	https://en.wikipedia.org/wiki/Power_outage
Blackout	https://en.wikipedia.org/wiki/Blackout
Brownout	https://en.wikipedia.org/wiki/Brownout
Port	https://en.wikipedia.org/wiki/Port
Dock (maritime)	https://en.wikipedia.org/wiki/Dock_(maritime)
Bridge	https://en.wikipedia.org/wiki/Bridge
Flight cancellation and delay	https://en.wikipedia.org/wiki/Flight_cancellation_and_delay
Delay	https://en.wikipedia.org/wiki/Delay
Electric power transmission	https://en.wikipedia.org/wiki/Electric_power_transmission

Table 16: 26 Most Popular Articles in 2012, 2013, and 2014 Comparator Group

Topic Keywords	Wikipedia Articles
Facebook	https://en.wikipedia.org/wiki/Facebook
Wiki	http://en.wikipedia.org/wiki/Wiki
Deaths in 2012	https://en.wikipedia.org/wiki/Lists_of_deaths_by_year#2012
One Direction	https://en.wikipedia.org/wiki/One_Direction
The Avengers (2012 film)	https://en.wikipedia.org/wiki/The_Avengers_(2012_film)
Fifty Shades of Grey	https://en.wikipedia.org/wiki/Fifty_Shades_of_Grey
2012 phenomena	https://en.wikipedia.org/wiki/2012_phenomenon
Google	https://en.wikipedia.org/wiki/Google
The Dark Knight Rises	https://en.wikipedia.org/wiki/The_Dark_Knight_Rises
The Hunger Games	https://en.wikipedia.org/wiki/The_Hunger_Games
Deaths in 2013	https://en.wikipedia.org/wiki/Lists_of_deaths_by_year#2013
Breaking Bad	https://en.wikipedia.org/wiki/Breaking_Bad
G-force	https://en.wikipedia.org/wiki/G-force
World War II	https://en.wikipedia.org/wiki/World_War_II
Youtube	https://en.wikipedia.org/wiki/YouTube
List of Bollywood Films 2013	https://en.wikipedia.org/wiki/List_of_Bollywood_films_of_2013
United States	https://en.wikipedia.org/wiki/United_States
Online shopping	https://en.wikipedia.org/wiki/Online_shopping
Java	https://en.wikipedia.org/wiki/Java
Alive	https://en.wikipedia.org/wiki/Alive
Deaths in 2014	https://en.wikipedia.org/wiki/Lists_of_deaths_by_year#2014
Climatic Research Unit email controversy	https://en.wikipedia.org/wiki/Climatic_Research_Unit_email_controversy
Amazon.com	https://en.wikipedia.org/wiki/Amazon.com
2014 FIFA World Cup	https://en.wikipedia.org/wiki/2014_FIFA_World_Cup
Ebola virus disease	https://en.wikipedia.org/wiki/Ebola_virus_disease
Game of Thrones	https://en.wikipedia.org/wiki/Game_of_Thrones

Appendix B

JONATHON W. PENNEY

Schulich School of Law, Dalhousie University
6061 University Ave, Halifax, NS, Canada, B3A 4M6
Phone: +(902) 830 3008 // Email: jon@dal.ca
Website: https://jonpenney.com

Dr. Jonathon Penney is a lawyer and social scientist who does research at the intersection of law, technology, and human rights. From the internet today to artificial intelligence and beyond tomorrow, his work aims to understand technology's role in public and private sector censorship, surveillance, and other emerging legal/regulatory practices. He has held appointments at the leading research centers in his field, including the Oxford Internet Institute, University of Oxford; Harvard's Berkman Klein Center for Internet and Society; Princeton's Center for Information Technology Policy; and the Massachusetts Institute of Technology's Media Lab. He is also the author of numerous publications and is a frequent speaker at technology law and policy conferences around the world.

Dr. Penney has studied law at Columbia Law School as a Fulbright Scholar and at Oxford as a Mackenzie King Scholar. He holds a doctorate in "Information, Communication, and the Social Sciences" from the interdisciplinary Oxford Internet Institute at the University of Oxford.

He has a particular expertise in measuring and exploring the impact of surveillance and other data driven and technology-focused regulatory activities, and is author of the book *Chilling Effects: Understanding the Impact of Surveillance and Other Technological Threats* (forthcoming in Cambridge University Press, 2019). His work has received international attention and coverage, including the *Washington Post*, *Reuters International*, *New York Times*, *Newsweek*, *TIME Magazine*, *NBC News*, *Forbes*, *Psychology Today*, *Le Monde*, *The Guardian*, *Freitag*, *Il Fatto Quotidiano*, *The Times of India*, *Indian Express*, *Jerusalem Post*, *Huffington Post*, *Politico*, *Slate*, *Motherboard*, *The Hill*, *The Index on Censorship*, as well as coverage by Pulitzer Prize winning journalist Glenn Greenwald in *The Intercept*.

CURRENT APPOINTMENTS / AFFILIATIONS

Schulich School of Law, Dalhousie University
Associate Professor, July 2018 – Present
Director, *Law and Technology Institute*, September 2017 – Present

Center for Information Technology Policy, Princeton University
Research Affiliate, September 2017 – Present

MIT Media Lab, Massachusetts Institute of Technology
Research Associate (Civil Servant Project), January 2018 – Present

Citizen Lab, Munk School of Global Affairs, University of Toronto
Research Fellow, September 2017 – Present

EDUCATION

Oxford Internet Institute, University of Oxford (Balliol College)
DPhil, Doctorate in Information, Communication, and the Social Sciences, January 2016
Thesis: Chilling Effects in the Internet Age: Three Case Studies
Committee: Dr. Victoria Nash (Oxford), Dr. Urs Gasser (Harvard), Dr. Joss Wright (Oxford)
Google Policy Fellow; SSHRC Doctoral Fellow; Centennial Scholar

Columbia Law School, Columbia University
LLM, Master of Laws, May 2009 (Harlan Fiske Stone Scholar; Fulbright Scholar; GLS Scholar)

Faculty of Law, University of Oxford (Wolfson College)
MSt, Master of Studies (Law), July 2007 (Lady Margaret Hall Award; Mackenzie King Scholar)
Associate-Editor, Oxford University Commonwealth Law Journal

Schulich School of Law, Dalhousie University
JD, Juris Doctorate, May 2003 (Dean's List; Tom Wilcox Award)
Editor of Reviews, Dalhousie Journal of Legal Studies

Faculty of Arts and Social Sciences, Dalhousie University
BA, Philosophy with minor Computer Science credits, May 2000 (Dean's List)

PAST APPOINTMENTS / EMPLOYMENT

Berkman Klein Center for Internet & Society, Harvard University
Berkman Fellow/Research Affiliate, September 2012 – September 2015

Citizen Lab, Munk School of Global Affairs, University of Toronto
Google Policy Fellow, May 2011 – September 2011

PVNets Project, Oxford Internet Institute, University of Oxford
Project Coordinator, September 2010 – September 2012

Faculty of Law, Victoria University of Wellington, Wellington, NZ
InternetNZ Cyberlaw Senior Research Fellow, September 2009 – September 2010

Regulatory Division, Ontario Regional Office, Department of Justice, Toronto
Litigation Counsel, September 2004 – September 2008

PUBLICATIONS

Books

"Chilling Effects: Understanding the Impact of Surveillance and Other Technological Threats" Cambridge University Press, forthcoming 2019

Articles

"The Expressive Value of Cyber-Stalking Laws" (2019) Fordham Law Review ____, forthcoming (with Danielle Citron)

"Privacy, Chilling Effects, and Personalized Legal Automation: The DMCA as an Empirical Case Study" (2019) Stanford Technology Law Review____

"Chilling Effects and the GDPR" (2019) European Law Journal ___, forthcoming (**peer reviewed**)

"Advancing Human Rights-by-Design in the Dual-Use Technology Industry" (with Lex Gill, Sarah McKune, and Ron Deibert), (2019) Columbia Journal of International Affairs, forthcoming (**peer reviewed**)

"Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study", (2017) 6(2) Internet Policy Review 1 (**peer reviewed**)

- Invited to write op-ed discussing paper's findings for *Slate*; research has also received coverage from *WIRED Magazine*, *Global Voices' Netizen Report*, *Slate France*, *Business Insider*, *Privacy Weekly*, European Digital Rights' *EDRi-Gram Report*, and Columbia University's *The Education Lab*.
- Top ten most downloaded article in July 2017 for multiple Social Science Research Network (SSRN) subject areas, incl. "Cyberspace Law", "Information Privacy Law" and "National Security Law".

"Chilling Effects: Online Surveillance and Wikipedia Use", (2016) 31 Berkeley Technology Law Journal 117

- Received extensive media coverage internationally, including the *Washington Post*, *New York Times*, *Newsweek*, *Reuters*, *NBC News*, *Forbes*, *Huffington Post*, *Le Monde*, *Der Freitag*, *Times of India*, *Jerusalem Post*, *Russia Today*, *Daily Mail*, *ABC News Australia*, *The Pakistan Express Tribune*, etc, as well as coverage by Pulitzer Prize winning journalist Glenn Greenwald in *The Intercept*
- #1 most downloaded article on SSRN in the week of May 13th, 2016 and the #2 most downloaded in the week of May 6, 2016; #66 most downloaded in last 12 months

"The Cycles of Global Telecommunication Censorship and Surveillance", (2015) 35 University of Pennsylvania Journal of International Law 693

"Virtual Inequality: Challenges for the Net's Lost Founding Value", (2012) 10 Northwestern Journal of Technology & Intellectual Property 209

"Open Connectivity, Open Data: Two Dimensions of the Right to Seek, Receive, and Impart Information", (2012) 4 Victoria University of Wellington Law Review 1 (**peer reviewed)**

"Internet Access Rights: A Brief History and Intellectual Origins" (2011) 38 William Mitchell Law Review 10 (**invited contribution**)

"Ivan Rand's Ancient Constitutionalism" (2010) 61 UNB Law Journal 43; (2010) 34 Manitoba Law Journal 43 (**peer reviewed)**

- This article won the **2011 Peter Oliver Prize in Canadian Legal History** (for "best article"), Osgoode Society for Canadian Legal History, Law Society of Upper Canada

"Technology and Judicial Reason: Digital Copyright, Secondary Liability, and the Problem of Perspective" (2010) 22 Journal of Intellectual Property 253 (2010) (**peer reviewed**)

"Understanding the New Virtualist Paradigm" (2009) 12 Journal of Internet Law 6

"Privacy and the New Virtualism" (2008) 10 Yale Journal of Law & Technology 194

"The Embarrassing Preamble? Understanding the 'supremacy of God' and the Charter" (2006) 39:2

University of British Columbia Law Review (with Robert Danay) 287 (**peer reviewed**)

"Deciding in the Heat of the Constitutional Moment: Constitutional Meaning and Change in the Quebec Secession Reference" (2005) 28:1 Dalhousie Law Journal 217 (**peer reviewed**)

"The Evolving Approach to Section 15(1): Diminished Rights or Bolder Communities?" (2005) 29 SUPREME COURT LAW REVIEW (2d) 137 (presented at the 8th Annual Constitutional Cases Conference at Osgoode Hall Law School, April 2005) (**peer reviewed**)

A Constitution for the Disabled or a Disabled Constitution? Toward a New Approach to Disability for the Purposes of Section 15(1)" (2003) 1 Journal of Law & Equality 83 (**peer reviewed**)

- Supporting document for World Health Organization and Pan-American Health Organization's 2004 International Convention on Intellectual Disabilities

Book Chapters / Contributions to Collective Works

"Cyber Security, Empiricism, and Human Rights: The Case of State and Non-State Surveillance" in Paul Cornish (eds), Oxford Handbook on Cyber Security (Oxford University Press, forthcoming 2019) (**peer reviewed**)

"Canadian Privacy Law and the Post War Freedom of Information Paradigm" in Gloria González Fuster, Rosamunde van Brakel and Paul De Hert (eds, Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics (Edgar, forthcoming 2018) (**peer reviewed**)

"*Zeran v AOL*'s Chilling Effect Claims" in Eric Goldman, ed, *Zeran v America Online 20 Years Later: A Compendium* (forthcoming 2018)

"Trade Secrets as Intellectual Property: Three Questions," in Mistrale Goudreau, Margaret Ann Wilkinson, & Florian Martin-Bariteau, eds, *New Paradigms in the Protection of Inventiveness, Data and Signs: Changing Perceptions of the Role of Intellectual Property* (Toronto: Irwin Law, forthcoming 2018) (**peer reviewed)**

Copyright's Media Theory and the Internet: The Case of the Chilling Effects Doctrine," in Courtney B Doagoo, Mistrale Goudreau, Madelaine Saginur & Teresa Scassa, eds, *Intellectual Property for the 21st Century: Interdisciplinary Perspectives on Intellectual Property Law* (Toronto: Irwin Law, 2013) (R) (**peer reviewed)**

Essays / Reports / Working papers

"Planet Netsweeper", Citizen Lab Research Report No. 2018-3, Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto, 2018

- This report documented how a Canadian company Netsweeper's web filtering technology has been used by oppressive governments around the world to facilitate censorship and other human rights abuses around the world received widespread media attention in Canada, including a special feature coverage on *CBC's The National*, the broadcaster's flagship national news program.

"Children and Cyberwar: Victimization and Protection" in Dustin Johnson, ed, *Allons-Y: Theory Into Action*, vol 2 (Halifax: The Roméo Dallaire Child Soldiers Initiative, August 2017).

"Can Cyber-Harassment Laws Encourage Online Speech?" in *Harmful Speech Online: At the Intersection of Algorithms and Human Behavior*, Berkman Klein Center Research Publication/Report, Berkman Klein Center for Internet & Society, Harvard University, 2017

"Chilling Effects and the DMCA: Comments in Response to Notice of Inquiry", submission to the U.S. Copyright Office for its Study of Section 512 of Title 17, United States Code (the Digital Millennium Copyright Act), March 30, 2016

"Warrant Canaries Beyond the First Amendment" in *Internet Monitor 2014*: *Reflections on the Digital World: Platforms, Policy, Privacy, and Public Discourse*, Berkman Klein Center Research Publication/Report, Berkman Klein Center for Internet & Society, Harvard University, 2014

"Code is Law, But Law is Increasingly Determining the Ethics of Code" in *Internet Monitor 2014: Reflections on the Digital World: Platforms, Policy, Privacy, and Public Discourse*, Berkman Klein Center Research Publication/Report, Berkman Klein Center for Internet & Society, Harvard University, 2014

"Communications Disruption and Censorship Under International Law", Free and Open Communications on the Internet (FOCI) Working Paper No. 9, USENIX Security Symposium, Advanced Computing Systems Association (ACSA), Bellevue, Washington, 2012 (**peer reviewed**)

Doctoral Thesis

"Chilling Effects in the Internet Age: Three Case Studies" (DPhil Thesis, University of Oxford, November 2015 [unpublished]) (**peer reviewed**)

- Successfully defended in November, 2015 with with no corrections, confirmed December 2016, and degree officially awarded in May 2018.

Public Policy / Commentary / Op-Eds

"How Surveillance Contributes to Fake News", Freedom to Tinker Blog, Center for Information Technology Policy, Princeton University, November, 2018 (forthcoming)

"(Mis)Conceptions about the Impact of Surveillance", Freedom to Tinker Blog, Center for Information Technology Policy, Princeton University, February 14, 2018

"Whose Speech Is Chilled by Surveillance?" Slate Magazine (Online), July 11, 2017

"How Surveillance Harms", Policy Options (Blog), December 12, 2016, Institute for Research on Public Policy (IRPP), Montreal, QC

"How can Atlantic Canada benefit from CETA?", Policy Options (Blog), October 25, 2016, Institute for Research on Public Policy (IRPP), Montreal, QC

"Harper's Charter Activism.", Policy Options (Blog), March 13, 2016, Institute for Research on Public Policy (IRPP), Montreal, QC

"An Amended Bill C-51 is Still a Problem: Lessons from the U.S.", Policy Options Magazine (May-June, 2015), Institute for Research on Public Policy (IRPP), Montreal, QC

"How Laws Are Increasingly Determining the Ethics of Code", Slate Magazine, January 9, 2015

"Constitutional Dialogue v2.0? Contentious Government Responses to the Supreme Court of Canada" (August 2014) Int'l J Const L Blog

"Doomed to Rely on the Mask", Policy Options Magazine , May-June, 2014) Institute for Research on Public Policy (IRPP), Montreal, QC

"Forget CSIS: It's the Political Parties that Own Our Privacy", Toronto Star, March 17, 2014

"Fighting Surveillance: What Canadian Companies Can Do" Citizen Lab (Blog), Munk School of Global Affairs, University of Toronto, February 13, 2014

"Deleting Revenge Porn", Policy Options Magazine , (Nov-Dec 2013), Institute for Research on Public Policy (IRPP), Montreal, QC

"Watching the Watchers: A Role for the ITU in the Internet Age", Cyberdialogue Blog, March 5, 2013, University of Toronto (**invited contribution)**

"Outsourcing Cyberwar", *The Future of Fighting and How the Canadian Military Must Adapt: Strategic Studies Working Group*, Canadian International Council & Canadian Defence and Foreign Affairs Institute, May 25, 2012 (**invited contribution**)

"Time to Get Serious About Cyber-Security", The Mark News (28 July 2011); Information Warfare Monitor, Citizen Lab, Munk School of Global Affairs, University of Toronto (July 2011)

"Countering the Anti-Counterfeiting Trade Agreement", Computer World, November 27, 2009

PRESENTATIONS / TALKS / INVITED LECTURES

Featured Speaker, "The First Amendment and Modern Surveillance", co-hosted by Yale Law School Information Society Project and Knight First Amendment Institute, Columbia University, November 14, 2018 (**invited**)

"Geneva Dialogue On Responsible Behaviour in Cyberspace ", Swiss Federal Department of Foreign Affairs, Geneva, Switzerland, November 1-2, 2018 (**invited**)

Session Discussant, "AI in Criminal Justice", DeepMind / Princeton CITP Limits of AI in Public Service Workshop, Center for Information Technology Policy, Princeton University, September 28, 2018 (**invited**)

"Measuring the Impact of Surveillance and Other Online Threats at Scale", The Emergence of Computational Legal Studies: The Promises and Challenges of Data-Driven Legal Research, First Annual Computational Legal Studies Workshop, Department of Law / Law and Technology Centre, University of Hong Kong, Hong Kong, June 28-29, 2018 (**invited**)

"Internet Surveillance: An Empirical and Comparative Case Study", 11th Annual Privacy Law Scholars Conference, George Washington University Law Center, Washington DC, May 30-31 2018 (**invited**)

Featured Speaker, RightsCon Summit (Toronto), May 16-18 2018, Toronto (**invited**)

Panelist, "Have We Entered a Brave New World of Global Content Takedown Orders?", Panel

organized by Harvard's Berkman Klein Center for Internet, RightsCon Summit, May 18, 2018, Toronto (**invited**)

Panelist, "Data Driven Decency: New, Collaborative Experiments to Diminish Online Hate and Harassment Online", Panel organized by Harvard's Berkman Klein Center for Internet and Society, RightsCon Summit, May 17, 2018, Toronto (**invited**)

Panelist, "The surveillance tool we love to carry: Cell phones searches and privacy in the evolving legal landscape", Panel organized by Canadian Civil Liberties Association, RightsCon Summit, May 16, 2018, Toronto (**invited**)

"Chilling Effects and the DMCA? An Empirical Case Study on Copyright Enforcement Online", Intellectual Property Law Discussion Group, Faculty of Law, University of Oxford, May 8 2018 (**invited**)

"Chilling Effects: How Laws and Surveillance Impact Us Online", CITP Luncheon Speaker Series, Center for Information Technology Policy, Princeton University, March 27, 2018 (**invited**)

"Mitigating the Impact of Automated Legal Processes on Internet Users", Civil Servant Research Summit, Center for Civic Media, MIT Media Lab, Cambridge, MA, January 28, 2018 (**invited**)

Presenter/Panelist, "Cybersecurity and Human Rights in the Online World", Political Science in the Digital Age: International Political Science Association (IPSA/AISP) International Conference, Hannover, Germany, December 4-6, 2017 (**invited**)

"Chilling Effects: How Laws and Surveillance Impact Us Online", OII Brown Bag Lunch Speaker Series, Oxford Internet Institute, University of Oxford, September 7, 2017 (**invited**)

"The Comparative Dimensions of Regulatory Chilling Effects Online", Rump Session Talk, 6th Annual Workshop on Free and Open Communications on the Internet (FOCI), USENIX Security Symposium, Advanced Computing Systems Association (ACSA), Vancouver, B.C., August 14, 2017

"Documenting the Impact of Surveillance on Civil Society" (with Tabasum Akseer), Connaught Summer Institute on Monitoring Internet Openness and Rights, Munk School of Global Affairs, University of Toronto, July 12, 2017 (**peer reviewed**)

"Trade Secrets for Open Societies: Some Modest Proposals For Reform", Sixth Annual Intellectual Property Scholars Workshop, University of Ottawa, Ottawa, May 10, 2017 (**peer reviewed**)

"The Comparative Dimensions of Chilling Effects Online", Internet Law Work-in-Progress Conference, Santa Clara High Tech Law Institute, Santa Clara Law School, Santa Clara, March 4, 2017

Presenter/Panel Discussant, "Cyberwarfare and International Humanitarian Law", 12th Annual International Humanitarian Law Conference, Schulich School of Law, Dalhousie University, January 27, 2017 (**invited**)

"Chilling Effects: Online Surveillance and Wikipedia Use", Privacy Law Workshop, Faculty of Law, University of Toronto, Toronto, November 19-20, 2016

Speaker Series Lecture, "Mass Hacking and the New Transparency: Legal and Public Policy Implications", Information Technology Policy Speaker Series, Computational Social Science Institute / Faculty of Computer Science, University of Massachusetts (Amherst), November 4, 2016 (**invited**)

"New Transparency Challenges", Connaught Summer Institute on Monitoring Internet Openness and Rights, Munk School of Global Affairs, University of Toronto, July 7, 2016 (**peer reviewed**)

Moderator / Discussant, "Privacy, the Internet, and the Right to be Forgotten", European Union Center for Excellence (EUCE) / Canadian International Council (CIC), Dalhousie U., April 20, 2016

"Chilling Effects: Insights on how laws and surveillance impact people online", Berkman Luncheon Series, Berkman Klein Center for Internet & Society, Harvard University, April 27, 2016 (**invited**)

"Chilling Effects and the DMCA? An Empirical Case Study on Copyright Enforcement Online", Internet Law Work-in-Progress Conference, New York Law School, New York City, March 5, 2016

Panel Discussant, "The Trans-Pacific Partnership: Economic, Social and Legal Implications for Atlantic Canada", Canadian International Council (CIC)/ Centre for Foreign Policy Studies, Dalhousie University, Delta Barrington, Halifax, March 2016

"Chilling Effects: Online Surveillance and Wikipedia Use", Cornell Law Society for Empirical Legal Studies (SELS) Global Junior Empirical Legal Scholars Workshop, Hebrew University, Jerusalem, Israel, December 2015 (**peer reviewed**)

Panel Discussant, "CETA: Intellectual Property Law Implications", CETA on the Brink? Post-Politics and the Finalization of the Canada-EU Trade Deal, European Union Center for Excellence (EUCE) / Canadian International Council (CIC), Dalhousie University, November 13, 2015

"Online Surveillance and Chilling Effects, 5th Annual Workshop on Free and Open Communications on the Internet", 2th Annual Free and Open Internet Communications (FOCI) Workshop, USENIX Security Symposium, Advanced Computing Systems Association (ACSA), Washington, D.C., August 10, 2015 (**invited**)

"Network Interference and Censorship Measurement: Ethical and Legal Issues", Connaught Summer Institute on Monitoring Internet Openness and Rights, Citizen Lab, Munk School of Global Affairs, University of Toronto, June, 27, 2015 (**peer reviewed**)

"Chilling Effects? Wikipedia Use and Online Surveillance", Fellows/Research Affiliates Discussion Group, Berkman Center for Internet & Society, Harvard University, May 6, 2015

"So... I Have This Genius Idea: Copyright, Trademarks, and Patents for Business and Innovative Ideas", (with Heather R Oke), Mixed Media Monthly: A Speaker Series About Art and the Business of Art, Artists Legal Information Society (ALIS), Art Gallery of Nova Scotia, April 16, 2015

"A Taxonomy of Chilling Effects", Internet Law Work-in-Progress Conference, Santa Clara High Tech Law Institute, Santa Clara Law School, Santa Clara, March 7, 2015

"Intellectual Property & NPOs: Issues, Suggestions, Best Practices", (with Alayna Kolodziechuk),

presentation to the Intellectual Property Law Section, Canadian Bar Association (Nova Scotia Branch), Pattersons LLP, January 16, 2015

"Internet Intermediaries and Corporate Transparency: The U.S. Experience", Connaught Summer Institute on Monitoring Internet Openness and Rights, Citizen Lab, Munk School of Global Affairs, University of Toronto, July, 29, 2014

"The Cycles of Global Telecommunications Censorship and Surveillance" University of Toronto—Osgoode Hall Law School Junior Scholars Workshop, Osgoode Hall Law School, April 25, 2014

Moderator / Discussant, "Transparency Reporting ", Transparency Working Group, Cyber Dialogue 2014: After Snowden, Whither Internet Freedom?, Canada Centre for Global Security Studies, University of Toronto, March 31, 2014

Moving Beyond Transparency Reporting: Internet Regulation & DMCA Parallels", Transparency Workshop, Boalt School of Law, University of California (Berkeley), November 19, 2013

Guest Lecture, "Copyright Law in Canada" Class: Law Information and Society (Prof. Bertrum MacDonald), School of Information Management, Dalhousie University, November 25, 2013

Panel Discussant, International Relations and Digital Technology Project, IDRTP Collective, Munk School of Global Affairs, University of Toronto, September 13, 2013 (**invited**)

"Early Weather Legal Report: Issues on the Horizon", 3rd Annual Workshop on Free and Open Communications on the Internet (FOCI), USENIX Security Symposium, Advanced Computing Systems Association (ACSA), Washington, D.C., August 13, 2013

"Welcome to Oz: Beyond a Black and White Debate on Internet Regulation (and Control)" (with Ryan Budish), Connaught Summer Institute on Monitoring Internet Openness and Rights, Citizen Lab, Munk School of Global Affairs, University of Toronto, July 22, 2013 (**invited**)

Panel Discussant, Transparency Reporting and Empirical Research in Intermediary Liability Standards Workshop, Institute for Information Law (IViR), University of Amsterdam, Amsterdam, NL, June 29, 2013 (**invited**)

Panel Discussant, Intermediary Liability and Freedom of Expression Roundtable, Institute for Information Law (IViR), University of Amsterdam, Amsterdam, NL, June 28, 2013 (**invited**)

Panel Discussant, "Cyberspace Governance: Exploring constitutive principles and values, today and into the future" Panel, Cyber Dialogue 2013: Governance without Governance in Cyberspace?, Canada Centre for Global Security Studies, University of Toronto, March 17-18, 2013 (**invited**)

"The Cycle of Global Telecommunications Technologies", Internet Law Work-in-Progress Conference, Santa Clara High Tech Law Institute, Santa Clara Law School, Santa Clara, March 16, 2013

"Internet Censorship and the Ghosts of Infowars Past", Berkman Center Luncheon Series, Berkman Center for Internet & Society, Harvard University, February 26, 2013 (**invited**)

"Doxxing, Hacker Culture, and the First Amendment" (with Molly Sauter), Berkman Fellows Hour, Berkman Center for Internet & Society, Harvard University, December 18, 2012

"Code as Speech and Other Challenges", Junior Scholars Workshop, Schulich School of Law, Dalhousie University, November 7, 2012

"Lessons for the Law & Politics of Internet Censorship Resistance Today" 2012-2013 Information Management Public Lecture Series, Faculty of Management, Dalhousie University, November 6, 2012 (**Invited**)

Commentator/Respondent, "Business Method Patents Are Coming to Canada", 42nd Annual Workshop on Consumer and Commercial Law, Schulich School of Law, Dalhousie , Oct 12-13, 2012

"Communications Disruption and Censorship Under International Law", 2nd Annual Free and Open Internet Communications (FOCI) Workshop of the 21st USENIX Security Symposium, Advanced Computing Systems Association (ACSA), Bellevue, Washington, August 8, 2012 (**peer reviewed**)

"Copyright's Media Theory and the Internet: The Case of the Chilling Effects Doctrine", Fifth Annual Intellectual Property Scholars Workshop, University of Ottawa, Ottawa, May 2012 (**peer reviewed**)

"Privacy Models for SenseCam (and Similar Research)" (with Paul Kelly), SenseCam2012: Third Annual Symposium, Exeter College, University of Oxford, April 3-4, 2012

Panel Discussant, Privacy and Financial Inclusion Conference, Birbeck College, University of London, London, UK, September, 2011

Panel Discussant/Moderator, "Copyright and Remix Culture", Remix Cinema Conference, University of Oxford, Oxford, UK, March 2011

"Open Connectivity, Open Data: Two Dimensions of the Right to Seek, Receive, and Impart Information in New Zealand", 2010 Annual Public Lecture in Cyberlaw, Faculty of Law, Victoria University of Wellington, Wellington, New Zealand, July 1, 2010 (**invited**)

Panel Discussant (and Co-organizer), "Public ACTA: Conference on the Anti-Counterfeiting Trade Agreement", Wellington Town Hall, Wellington, New Zealand, April 2010

Panel Discussant and Panel Co-Chair, "Copyright Future: Authors, Owners, Orphans, Users, and Repeat Infringers", New Zealand Centre for International Economic Law, Victoria University, October 2009 (**Invited**)

Panel Discussant, "Governance and Virtual Worlds", State of Play IV: Law and the Past, Present, and Future of Virtual Worlds, New York Law School, New York City, June 2009 (**invited**)

"The Emancipation Proclamation as a Constitutional Document", Cornell Law School Inter-University Graduate Conference, Cornell Law School, April 14, 2009

"The Evolving Approach to Section 15(1): Diminished Rights or Bolder Communities?" (with Roselyn J. Levine, Q.C.), 8th Constitutional Cases Conference, Osgoode Hall Law, York U. Toronto, April 2005

CURRENT GRANT FUNDED RESEARCH PROJECTS

PRINCIPAL INVESTIGATOR / CO-INVESTIGATOR (FUNDED)

Mitigating the Impact of Automated Enforcement Online
Princeton University / Massachusetts Institute of Technology / Dalhousie University

Fund: Artificial Intelligence Ethics & Governance Fund, MIT Media Lab
Amount: $154,736 CAD (125,000 USD) over 2 years (Fall 2017-2019)
Role: Co-Principal Investigator
Co-Investigators: Ethan Zuckerman, Associate Professor and Director, Center for Civic Media, MIT Media Lab; J. Nathan Matias, Postdoctoral Fellow, Princeton University; Merry Mou, a MIT Computer Science graduate student

This research project explores the impact of online platforms deploying algorithms and automated processes to enforce legal rights and obligations, monitor/surveil users, or police content and other online services, including testing legal, regulatory, and technological measures to mitigate negative side effects and, in the long run, protect people's rights and freedoms. We also expect to provide invaluable insights into how businesses and corporate platforms can more effectively employ these automated processes, while balancing business aims with user rights and consumer interests. Our methods are empirical, interdisciplinary, often collaborative with online platforms themselves, and use big data sources—like online platform data—and data analytics along with innovative and experimental research designs to do so. Our first case study in a series of such studies in collaboration tracks the impact of automated processes and "bots" enforcing copyrights online at mass scale under the U.S. Digital Millennium Copyright Act (DMCA). This study involves 100,000 social media users and documents the impact of these bots on users and platforms while testing different measures to mitigate any negative side effects like chilling effects and self-censorship. Other studies will look at automated content moderation on platforms, as well as biases in surveillance algorithms.

Toward a Public Interest Approach to Publicly Accessible Platform Data (FUNDED)
University of Ottawa / Dalhousie University / Ryerson University

Fund: Insight Grant, Social Sciences and Humanities Research Council (SSHRC)
Amount: $189,916 over 4 years (Fall 2018-2022)
Role: Co-Principal Investigator / Applicant
Co-Investigators: Teresa Scassa, Canada Research Chair in Information Law at University of Ottawa; and Pamela Robinson, Associate Professor, School of Urban and Regional Planning, Ryerson University

This is a multi-year SSHRC Insight grant funded project investigates the legal, ethical, and policy dimensions of publicly accessible platform data. This will include, among things, examining the issues of ownership, user rights, control, and privacy in relation to this data, and challenges raised by related emerging technologies and data practices like big data analytics, automated and algorithmic data scraping and processing, and automated platform content moderation. The project will confront issues of tort law, contract law, property law, as well as new and evolving forms of e-contracts, consumer protection, and commercial transactions

Connected Canada: Digital Citizenship in Canada Today (FUNDED)
University of Ottawa / Dalhousie University / University of British Columbia / Public Policy Forum

Fund: Connection Grant, Social Sciences and Humanities Research Council (SSHRC)
Amount: $24,592CAD over 1 year (Spring 2017-2018)
Role: Co-Principal Investigator / Applicant
Co-Investigators: Elizabeth Dubois, Assistant Professor, University of Ottawa; Alfred Hermida, Professor, School of Journalism, University of British Columbia; Florian Martin-Bariteau, Assistant Law Professor/Director, Center for Law and Technology, University of Ottawa

This is a multi-university, multi-partner SSHRC Connection grant used to fund a national conference to lay the foundations for a research agenda on "digital citizenship in Canada", including a significant technology law component. The October 2017 conference brought together academics across disciplines, policy makers, government officials, think tanks, civil society groups, and the private sector to investigate the internet Canada, including its history, emerging technologies, and applications, to understand what digital citizenship in Canada looks like, who is excluded from this vision, and how Canadian law and policy might respond.

PRINCIPAL INVESTIGATOR / CO-INVESTIGATOR (SUBMITTED)

Regulatory Gaps and Best Practices For a Rapidly Shifting Environment
Advanced Data Science Alliance (ADA)
Fund: Tri-Council Network Centres of Excellent Grant
Amount: $25 million over 5 years
Role: Co-Principal Investigator
ADA Scientific Co-Leads: Kelly Lyons (University of Toronto), Eleni Stroulia (University of Alberta), and Stan Matwin (Dalhousie University)
Theme Co-Leads: Lisa Austin, Professor of Law, University of Toronto; David Lie, Professor of Computer Engineering
Co-Principal Investigators: David Lyon, Professor of Sociology and Queen's Research Chair in Surveillance Studies, Queen's University; Ian Kerr, Professor of Law and Canada Research Chair, University of Ottawa

This project will be part of a large scale Tri-Council Networks Centres of Excellence project led by the Advanced Data Science Alliance (ADA), a multi-sectoral and trans-disciplinary national research network that, in partnership with industry and the public sector, will identify and address barriers to data-related innovation and enhance competitiveness in key sectors of the Canadian economy. There are 8 sub-themes in network, with law and policy addressed within the "Ethical, Accountable Technologies" sub-theme. The work on this sub-theme is led by University of Toronto's Lisa Austin and David Lie and aims to develop multidisciplinary approaches to new regulatory and ethical challenges for advanced data science methods, with special focus on emerging technologies like AI and machine learning, through research and training based on notions of corporate social responsibility and data justice. All Co-Leaders and Principal Investigators for the theme project are committed to multidisciplinary work and have academic backgrounds spanning law, philosophy, sociology, economics, computer engineering, and computer science. As well, the British Columbia, Alberta, and Federal Privacy Commissioners Offices will act as receptor partners for the grant and will help assist, support, and develop relating research, networking, and training opportunities.

COLLABORATOR

Internet Monitor and Transparency Project
Berkman Klein Center for Internet and Society, Harvard University

Fund: MacArthur Foundation
Amount: $1,242,760CAD over 5 years ($400,000USD 2013-2015; $600,000USD 2015-2018)
Role: Collaborator
Principal Investigator: Urs Gasser, Professor, Harvard Law School and Executive Director, Berkman Klein Center for Internet and Society, Harvard University

The award supports an applied research agenda to inform and shape policy development for governments and technology companies related to privacy, transparency, innovation, and security. The three areas of engagement include: 1) reducing privacy and security risks raised by private sector and government data sharing; 2) improving transparency and accountability associated with data acquisition and use by private companies; and 3) addressing harmful speech online. Currently building collaborative partnerships with private sector internet companies to broaden and standardize transparency reporting, to allow research on released data (in progress), including the impact of corporate surveillance and data disclosure. This also includes contributing to a large multi-faceted report on the impact of harmful speech online.

The Digital Copyright Takedown Project
Boalt School of Law, University of California (Berkeley) / Columbia University

Fund: Alfred P. Sloane Foundation and the Berkeley Digital Library Copyright Project
Amount: $1,517,924CAD over 6 years ($836,849USD 2011-2013; $384,565USD 2014-Present)
Role: Collaborator
Principal Investigators: Jennifer Urban, Professor, Boalt School of Law, University of California (Berkeley); Karaganis, American Assembly, Columbia University

A research project led by Jennifer Urban (Faculty of Law, UC Berkeley) and Joe Karaganis (American Assembly, Columbia University) that brings together range of scholars and researchers from universities around the world to collaborate on large-scale research project exploring intellectual property, copyright, and other intermediary liability enforcement systems and measures employed globally.

RECENT PAST GRANT FUNDED RESEARCH PROJECTS

PRINCIPAL INVESTIGATOR

CETA's Privacy and IP Implications for Canada
European Union Center for Excellence, Dalhousie University

Fund: European Commission
Amount: $10,000CAD (2015)
Role: Co-Principle Investigator / Applicant
Co-Investigators/Co-Applicant: Ruben Zaiotti, Director, European University Center for Excellence, Dalhousie University

This project, funded by the European Union (EU) (grant for funds succeeded via grant application in coordination with the European Union Center for Excellence at Dalhousie), examines the privacy and intellectual property law implications of the Comprehensive Economic Trade Agreement (CETA) between Canada and the EU. This grant funded participation in a symposium (examining trademark law/geographical indications under CETA), organizing/holding a conference on Europe's Right to be Forgotten (RTBF) in Canada,

and a report on CETA's implications for Canadian intellectual property laws.

Chilling Effects in the Digital Age: Three Case Studies
Doctoral Thesis, Oxford Internet Institute / Balliol College, University of Oxford

Funds: Doctoral Fellowship, Social Sciences and Humanities Research Council; Canada; Balliol College Graduate Student Bursary Fund; Canadian Centennial Scholarship Fund
Amount: $80,000CAD over 4 years ($20,000CAD/year, 2010-2014) along with miscellaneous amounts from year to year from the Balliol College scholarship and bursary funds;
Role: Principal Investigator / Applicant

My doctoral dissertation at Oxford explored the phenomena of regulatory chilling effects online through three empirical legal case studies, one involving the impact of online surveillance, another on the impact of the digital copyright enforcement online, and another survey-based study comparing the impact of different forms of online state actions/regulation. Primarily funded a SSHRC Doctoral Fellowship (converted from a CGS to take abroad).

PROJECT COORDINATOR

Privacy Value Networks (PVNets) Project
Oxford Internet Institute, University of Oxford

Fund: Engineering and Physical Sciences Research Council (ESPRC), United Kingdom
Amount: $2,534,953CAD over 4 years (£1,553,090, 2008-2012).
Role: Project Coordinator
Principal Investigator: Ian Brown, Professor, Oxford Internet Institute, University of Oxford
Collaborators: MA Sasse, Professor, University College of London; TNH Henderson, Professor, University of St. Andrew

A public and private sector research collaboration, funded by the UK's Engineering & Physical Sciences Research Council (EPSRC), on data privacy involving multiple universities and consulting firms. Coordinated all aspects of the project, including facilitating collaboration and communication among participants, organizing and chairing project meetings, formulating and administering project plan, monitoring deadlines, drafting and formulating project status reports, funding agency communications and relations, financial reporting, contracts, project deliverables, and their dissemination.

RESEARCH ADVISORY WORK

Ethics Feedback Panel for Networking and Security Research
Research Ethics Project, Microsoft Research, Cambridge, MA

Role: Panel Member / Collaborator
Principal Investigators: Stuart Schechter, Microsoft Research, Cambridge, MA and Bendert Zevenbergen, Postdoctoral Fellow, Princeton's Center for Information Technology Policy

The Networking and Security Research Ethics Feedback Panel (EFP) is an initiative led by Microsoft Research's Stuart Schechter. The EFP is a forum populated by volunteer experts in privacy, surveillance, and network security research that aims to help researchers identify ethics-related risks from their experiments and reduce these risks. The EFP encourages researchers to submit their research proposals for feedback prior to submitting them for

institutional review, so that they may integrate risk-reduction measures suggested by panelists and use panelists' feedback to inform institutional reviewers.

SELECTED MEDIA SPOTS / PRESS COVERAGE

I have been interviewed and quoted in media as an expert and my research received press coverage nationally and internationally, including the *Washington Post*, *New York Times*, *Newsweek*, *Reuters*, *TIME Magazine*, *NBC News*, *Le Monde*, *The Guardian*, *Forbes*, *Huffington Post*, *Politico*, *Slate*, *Motherboard*, *The Hill*, *The Globe and Mail*, *Toronto Star*, *CBC News*, *Global News*, *The Daily Mail*, *The Index on Censorship*, *Der Freitag*, *Il Fatto Quotidiano*, *The Times of India*, *Indian Express*, *Jerusalem Post*, as well as coverage by Pulitzer Prize winning journalist Glenn Greenwald in *The Intercept*.

Research covered in Lily Newman "The ACLU's Biggest Roadblock to Fighting Mass Surveillance" **WIRED Magazine**, June 29, 2018

Research covered in A.J. Marsden and William Nesbitt, "I Spy with My Little Eye: The Origins and Effects of Mass Surveillance" **Psychology Today**, November 6, 2017

Research covered / quoted in Tilman Bayer, "The chilling effect of surveillance on Wikipedia readers, and other recent research" in **Wikipedia Research Newsletter**, Vol 7:4, July 24 2017

Research covered / quoted in Peggy Sastre, "Sur Internet, les femmes et les jeunes s'autocensurent le plus", **Slate France**, July 16, 2017

Research covered in Tonya Riley, "Future Tense Newsletter: Trump's Idea for a U.S.-Russia Cybersecurity Unit Is Unbearably Dumb", **Slate Magazine**, July 12, 2017

Research covered in Gary Natriello, "The Chilling Effects of Surveillance", Ed Lab, Teachers College, **Columbia University**, July 12, 2017

Research covered in News, "Women and young people are hurt the most by internet surveillance — and it's getting worse", **Business Insider**, July 8, 2017

Research cited in John Naughton, "Google, not GCHQ, is the truly chilling spy network", **The Guardian**, June 18, 2017

Research recommended in Global Voices Advocacy, "In 'State of Emergency,' Internet Shutdowns Leave Ethiopians, Venezuelans Struggling to Connect", **Netizen Report**, June 1, 2017

Research covered / quoted in Jonathan Shaw, "The Watchers: Assaults on Privacy in America", **Harvard Magazine**, January-February, 2017

Research mentioned in Cynthia Wong, "The Dangers of Surveillance in the Age of Populism", **Newsweek**, February 2, 2017

Research covered in George Bowden, "Nine Important Stories of the Year That Slipped Under the Radar", **Huffington Post** (United Kingdom), December 27, 2016

Research mentioned in Henry Peck, "Speech Restrictions Cannot Be Wordplay", **Human Rights**

Watch (Dispatches Blog), October 26, 2016

Quoted in James Bradshaw, "Turkey's Erdogan uses FaceTime, social media to thwart military coup", **Globe and Mail**, July 26, 2016

Research covered in The Mackenzie Institute, "The Chilling Effect – How Mass Surveillance is Changing Your Online Behavior" (Video), June 26, 2016

Radio Interview (with host Dan Jones), "The Chilling Effect", **Radio Berkman 237**, Berkman Klein Center for Internet & Society, Harvard University, May 18, 2016

Research noted in Janus Kopfstein, "Lack of Online Privacy Has Chilling Effect, U.S. Department of Commerce Says", **Motherboard VICE**, May 14, 2016

Research covered in Brady Dale, "Humans Are the Best Sensors—Pairing Flickr With the News", **New York Observer**, May 6, 2016

Research covered / quoted in Annika Kremer, "Studie beweist Selbstzensur durch Überwachung", **Der Freitag** (Germany), May 6, 2016

Research covered / quoted in Tim Cushing, "The Chilling Effect Of Mass Surveillance Quantified", **Techdirt**, May 2, 2016

Research covered in News, "Traffic to Wikipedia Terrorism Entries Plunged After Snowden Revelations", **The Daily Mail** (United Kingdom), May 1, 2016

Research covered in News, "Study: Traffic to Wikipedia Terrorism Entries Plunged After Snowden Revelations", **Jerusalem Post**, May 1, 2016

Research covered in News, "Traffic to Wikipedia Terrorism Entries Plunged", **The Nation (Pakistan)**, May 1, 2016

Research covered / quoted in, News, "People Too Afraid To Search Privacy-Sensitive Topics After Snowden Revelations— Oxford Study", **Russia Today**, May 1, 2016

Research covered / quoted in Joshua Kopstein, "Snowden's Leaks Made People Less Likely to Read About Surveillance", **Motherboard**, April 30, 2016

Research covered in Yael Grauer, "Traffic to Wikipedia Entries Related To Terrorism Plummeted In Light of NSA Spying", **Forbes**, April 29, 2016

Research covered in Le Monde Pixels, "Traffic Après les révélations Snowden, moins de visites sur les pages Wikipédia sensibles", **Le Monde (France)**, April 29, 2016

Research covered in Amaelle Guiton, "Web : de la surveillance de masse à l'autocensure", **Libération (France)**, April 29, 2016

Research covered / quoted in Nieuws, "Als de staat meeluistert zijn burgers minder vrij", **Joop VARA** (Netherlands), April 29, 2016

Research covered / quoted in Glenn Greenwald, "New Study Shows Mass Surveillance Breeds Meekness, Fear, and Self-Censorship", **The Intercept**, April 28, 2016

Research covered / quoted in Marius Jorgenrud , "Færre leser om terror på Wikipedia etter Snowden-avsløringene, **Digi No** (Norway), April 28, 2016

Research covered in "Traffic to Wiki Terrorism Entries Plunged After Snowden Leaks", **Hindustan Times** (India), April 28, 2016

Research covered in News, "Traffic to Wikipedia terrorism entries plunged after Snowden revelations, study finds", **Reuters Africa**, April 28, 2016

Research covered in News, "Denúncias de Snowden fizeram cair tráfego de páginas sobre terrorismo na Wikipedia, entenda", **Tudo Celular** (Brazil), April 28, 2016

Research covered in Giulio Cupini and Fabio Scalet, "Privacy, lo spionaggio ci rende più ignoranti", **Il Fatto Quotidiano** (Italy), April 28, 2016

Research covered in News, "Internet Users Avoid Searching for 'Terrorism' on Web After Snowden Leak", **Sputnik News** (Russia), April 28, 2016

Research covered in Tim Starks, "Morning Cyber-Security Report", **Politico**, April 28, 2016

Research covered / quoted in Jeff Guo, "New Study: Snowden's disclosers about NSA spying had a scary effect on free speech", **Washington Post**, April 27, 2016

Research covered / quoted in Joseph Menn, "Traffic to Wikipedia terrorism entries plunged after Snowden revelations, study finds", Reuters (International), April 27, 2016

Research covered in NBC News Report, "Traffic to Wikipedia Terrorism Entries Plunged After Snowden Revelations", **NBC News**, April 27, 2016

Research covered / quoted in "Wikipedia Terrorism Entries Traffic Fell After Snowden NSA Reveal", **Newsweek Magazine**, April 27, 2016

Research covered in News, "Traffic to Wikipedia Terrorism Entries Plunged After Snowden Revelations, Study Finds", **The New York Times**, April 27, 2016

Research covered / quoted in Cory Bennett, "Snowden revelations had chilling effect on web browsing", **The Hill**, April 27, 2016

Research covered / quoted in Rudy Takala, "Study: Snowden leaks have made web users paranoid about what they browse", **Washington Examiner**, April 27, 2016

Research covered / quoted in Andrew Blake, "NSA surveillance has had a chilling effect on Internet browsing: report", **Washington Times**, April 27, 2016

Research covered in "Wikipedia traffic to terrorism entries plunge after Snowden revelations, study finds", **Business Insider**, April 27, 2016

Research covered / quoted in J. Nate Matias, "The Effects of Surveillance and Copyright Law on Speech: Jon Penney at Berkman", **MIT Center for Civic Media** (Blog), Massachusetts Institute of Technology, April 27, 2016

Research covered in News, "Consultas sobre terrorismo en Wikipedia bajan tras el escándalo de

Snowden: estudio", **Radio Fórmula** (Mexico), April 27, 2016

Research covered / quoted in Torsten Kleinz, "Studie zu Chilling Effects: Wikipedia-Artikel zu Terrorismus werden weniger gelesen", **Heise Online** (Germany), April 27, 2016

Research covered in News, "Wikipedia Pages on Terror See Traffic Plunge Post Snowden Leaks", **The Times of India**, April 27, 2016

Research covered in News, "Traffic to Wikipedia Terrorism Entries Plunged After Snowden Revelations: Reports", **Indian Express**, April 27, 2016

Research covered in News, "Security Revelations See Fall in Web Traffic – Study", **Otago Daily** (New Zealand), April 27, 2016

Research covered in News, "Wikipedia traffic to terrorism entries plunge after Snowden revelations, study finds", **ABC News** (Australia), April 27, 2016

Research covered in News, "Traffic to Wikipedia Terrorism Entries Plunged After Snowden Revelations, Study Finds", **Eyewitness News** (South Africa), April 27, 2016

Research covered in Esti Utami, "Setelah Pengakuan Snowden Pengakses Info Terorisme Menurun", **Suara News** (Indonesia), April 27, 2016

Research covered in News, "Wikipedia traffic to terrorism entries plunge after Snowden revelations, study finds", **Gulf Daily News** Online (Bahrain), April 27, 2016

Research covered in News, "Wikipedia traffic to terrorism entries plunge after Snowden revelations, study finds", **The Peninsula (Qatar)**, April 27, 2016

Research covered in "Traficul către paginile de Wikipedia dedicate terorismului a scăzut semnificativ după dezvăluirile lui Snowden (studiu)", **Agerpres** (Romania), April 27, 2016

Research covered in News, "Traffic to Wikipedia Terrorism Entries Plunged After Snowden Revelations, Study Finds", **The Express Tribune** (Pakistan), April 27, 2016

Research covered in News, "Traffic to Wikipedia terrorism entries plunged after Snowden revelations", **Free Malaysia Today**, April 27, 2016

Research covered in News, "Traffic to Wikipedia Terrorism Entries Plunged After Snowden Revelations, Study Finds", **Standard Media** (Kenya), April 27, 2016

Quoted in Robin Levinson King, "FCC met with Canadian researcher to understand CRTC", The **Toronto Star**, February 26, 2015

Quoted in Rebecca Lau, "Internet users receive illegal downloading notices, but what do they mean?", **Global News**, February 24, 2015

Quoted in Robin Levinson King, "Canadian viewers will get to see U.S. ads during 2017 Super Bowl", **The Toronto Star**, January 29, 2015

Quoted in M Donovan, "Failure to Connect: Nova Scotia's Digital Divide", **The Coast**, Oct 1, 2015

Quoted in: Sam Frizell, "Here's What Facebook Can Do With Your Personal Data in the Name of Science" **TIME Magazine** (July 7, 2014)

Quoted in "Elections Bill Exacerbates Lack of Privacy, Political Parties Micro Target Voters", The **Hill Times**, April 7 2014

Television Interview / Quoted in "NS Government hires Ontario lawyers to fight Bluenose II lawsuit:", **Global News (**TV), September, 2013

Quoted extensively in: Anonymous, "The Great Firewall of China", **Index on Censorship Uncut** Blog (15 March 2013)

ACADEMIC HONOURS AND DISTINCTIONS

2016 –
- Best Moot Team (Dalhousie), Best Oral Advocate (Gabby Lemoine, Dalhousie), Harold G. Fox IP Moot Competition, Toronto (Moot Team Coach / Supervisor)
- Research Affiliation, Civil Servant Project, MIT Media Lab (2018 – Present)
- Research Affiliation, CITP, Princeton University (2017 – Present)
- Research Fellowship, Citizen Lab, University of Toronto (20,000CAD) (2017 – 2018)

2013 – 2015
- Nomination, Law Students Association Award for Excellence in Teaching Law, Schulich School of Law, Dalhousie University (Spring 2015)
- Centennial Scholarship, Centennial Scholarship Fund, London, U.K. (2014)
- Research Affiliation, Berkman Klein Center for Internet and Society, Harvard University (2013 – 2015)

2012 – 2013
- Berkman Fellowship, Berkman Klein Center for Internet and Society (now Berkman Klein Center), Harvard University (2012 – 2013)
- Research Fellowship, Citizen Lab, University of Toronto (2012 – 2017)
- Research Affiliate, The Takedown Project, UC Berkeley Law; Eisenhower Institute, Columbia University (2013 – Present)

2010 – 2012
- Google Policy Fellowship, Citizen Lab, University of Toronto (7,500USD) (2011)
- 2011 Peter Oliver Prize in Canadian Legal History (c/o Osgoode Society/Law Society of Upper Canada) for "best article on Canadian legal history"
- Invited to give 2010 Annual Public Lecture on Cyberlaw at Victoria University of Wellington Law School, Victoria University, Wellington, New Zealand
- Social Sciences & Humanities Research Council Canadian Graduate Scholarship (converted to a Doctoral Fellowship to use abroad) (2010 – 2014)

2006 – 2009
- Harlan Fiske Stone Scholar Distinction, Columbia Law School (2009)
- Fulbright Scholarship, Canada-U.S. Fulbright Foundation (2008 –2009)
- Columbia Graduate Legal Studies Scholarship, Columbia Law School (2008 –2009)
- Lady Margaret Hall Award, University of Oxford (top student in the college's Social Sciences Division) (2007)
- Mackenzie King Travelling Scholarship, Mackenzie King Trust (2006 –2007)

2001 – 2003
- Tom Wilcox Award, Schulich School of Law, Dalhousie University (2003)
- Dean's List Distinction, Schulich School of Law, Dalhousie University (2003)
- Reviews Editor, Dalhousie Journal of Legal Studies, Dalhousie Law (2003)
- Dean's List Distinction, Dalhousie University (2000)

TEACHING

2012 – **Schulich School of Law, Dalhousie University**

Law and Technology (2014 – Present)
Upper Year Major Paper Seminar, Fall Term

Contract Law – Fall and Winter (2012— Present)
Mandatory First Year Course, Full Year)

Harold G. Fox Intellectual Property Moot (Coach/Supervisor) (2017 – Present)
Won top moot team and top mooter in first year participating (2017-2018)

Aboriginal and Indigenous Law in Context – (Facilitator) (2018 – Present)
First year 2 credit mandatory intensive course; I will facilitate, review, and engage student presentations as part of the Winter term module

Intellectual Property Law – (2012 – 2016)
Upper Year General Survey Course, Winter Term

2009 – 2010 **Faculty of Law, Victoria University of Wellington**

Internet Law and Regulation – Spring 2010
Upper Year / Graduate Seminar

GRADUATE SUPERVISION

Supervisor / Second Reader

Maria Dugas (Canada), LLM student, Thesis: "The Theoretical Case Against Criminalized Copyright Infringement in Canada" (Completed: 2017)

Ashwin Krishnan (India), LLM student, Thesis: "Towards an Effective Regime Against Online Copyright Infringement in India" (Completed: 2016)

Olefunke Salami (Nigeria), LLM student, Thesis: "Privacy Protection for Mobile Health (mHealth) in Nigeria" (Completed: 2015)

Farhan Raouf (Pakistan), LLM student, Thesis: "Modernizing Pakistan's Blasphemy Laws as Hate Speech" (Completed: 2014)

Directed Research Papers

Manal Alotiaba (Saudi Arabia), LLM student, "Anti -Cybercrime Law, Revenge Porn and Cyber Misogyny: A Comparative Analysis of the KSA, Canada, Egypt, and Pakistan" (Completed: 2018)

Liam Randhawa (Canada), "Luxury Fashion Brand Accessories: Perverting Trademark Law Theories" (Completed: 2016)

Examiner

Nick Hooper (Canada), LLM student, "Language's Empire: The Linguistic Foundations of Administrative Law" (Expected completion: Fall 2018)

PROFESSIONAL SERVICE

University Committees / Leadership

Director, Law and Technology Institute (September 2017 – Present)

Senator (Law School Rep.), Senate Standing Committee, Dalhousie U. (September 2017 – Present)

Chair, Information Technology Committee (2014 – Present)

Member: Research Committee (2012 – Present)

Member, Information Technology Committee (2012 – Present)

Associate, Jean Monnet European Union Centre for Excellence (2012 – Present)

Steering / Program Committees / Conference Chair

Steering Committee Member, Free and Open Communications on the Internet Workshop, USENIX Security Symposium, Advanced Computing Systems Association (2017– Present)

Co-Chair (with Nicholas Weaver of UC Berkeley), Free and Open Communications on the Internet Workshop (FOCI), USENIX Security Symposium, Advanced Computing Systems Association (ACSA) (2016-2017).

Program Committee: Free and Open Communications on the Internet Workshop, USENIX Security Symposium, Advanced Computing Systems Association (ACSA) (2012-2016)

Research Advisory Work

Member, Ethics Feedback Panel for Networking and Security Research, The Research Ethics Project, Microsoft Research, Cambridge, MA (2013 – Present)

PROFESSIONAL DESIGNATIONS AND MEMBERSHIPS

Bar Admissions

Law Society of Upper Canada, Province of Ontario, Canada (Year of Call: 2004)

New York State (Year of Call: 2013)

Professional Certifications

Certificate, Professional Training for Social Scientists, Saïd Business School, Oxford University

Certificate of Completion, Tri Council Policy Statement: Ethical Conduct for Research Involving Humans Course on Research Ethics (TCPS2: CORE)

Research Affiliations

Center for Information Technology Policy, Princeton University (2017 – Present)

Civil Servant Project, MIT Media Lab, Massachusetts Institute of Technology (2018 – Present)

Citizen Lab, Munk School of Global Affairs, University of Toronto (2012– Present)

Takedown Project, UC Berkeley Law / Columbia University (2012– Present)

Associate, Jean Monnet European Union Centre for Excellence (2012 – Present)

Organizations and Professional Membership

International Political Science Association (IPSA), Paris (since 2017).

Electronic Frontier Foundation (EFF), San Francisco, California (since 2012)

InternetNZ, Internet Society of New Zealand, (since 2009)

Oxford Union Debating Society (OUDS), University of Oxford (since 2007)

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

Plaintiff's Exhibit 3

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, *Plaintiff*, v. NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE, *et al.*, *Defendants*.	No. 1:15-cv-00662-TSE

DECLARATION OF MICHELLE PAULSON

I, Michelle Paulson, declare:

1. I am a resident of San Francisco, California, over the age of eighteen. I have personal knowledge of the facts stated in this declaration and if called to testify I could and would testify competently thereto. I am providing this declaration in my capacity as a former employee of and current consultant to the Wikimedia Foundation, Inc. ("Wikimedia").

2. I am currently General Counsel at Redacted, and I serve as a consultant to Wikimedia. From July 2016 to May 2017, I was Interim General Counsel of Wikimedia, and from July 2015 to May 2017, I was a Legal Director for Wikimedia. I served as Senior Legal Counsel from November 2014 to July 2015, and as Legal Counsel from March 2010 to November 2014. I received my B.A. from the University of California, Berkeley and my J.D. from the University of California, Hastings. I am a member of the bars of the states of California and New York.

3. During my time with the Wikimedia legal team, I helped update and create Wikimedia's policies and guidelines related to user privacy and data retention. I also worked

closely with Wikimedia's engineers who were responsible for operationally implementing Wikimedia's data security protocols.

I. BACKGROUND

A. The Wikimedia Foundation

4. Wikimedia is a 501(c)(3) nonprofit charitable organization based in San Francisco, California, dedicated to encouraging the growth, development, and distribution of multilingual educational content, and to providing the full content of these "wiki"-based projects to the public free of charge.[1] Wikimedia operates twelve free-knowledge projects ("Projects") on the Internet, including Wikipedia, the world's largest and most popular encyclopedia.

5. Wikimedia provides the technical infrastructure for the Projects, which are primarily hosted on Wikimedia servers in Virginia, Texas, California, and Illinois. In addition, Wikimedia develops software and provides tools for others to build software platforms; develops mobile phone applications and has entered into partnerships with telecommunications companies; administers grants to support activity that benefits the Wikimedia user community and movement; provides administrative support to grantees; works with community members to organize conferences and community-outreach events globally; and engages in advocacy on issues that affect the Wikimedia community—which, at its broadest level, consists of individuals who access or contribute to the body of knowledge comprising the twelve Projects.

B. Wikipedia and Wikimedia's Other Free Knowledge Projects

6. The best-known of Wikimedia's Projects is Wikipedia—a free, multilingual Internet encyclopedia that is one of the most-visited websites in the world and one of the largest

[1] A "wiki" is a web application that allows collaborative modification, extension, or deletion of its content and structure.

collections of shared knowledge in human history. As of February 2018, the site has grown to contain more than 47 million articles in over 288 languages, and in 2017 it received more than 1 billion unique device visits each month. Wikipedia's content is collaboratively researched and written by millions of volunteers, many of whom choose not to identify themselves, and is in most instances open to editing by anyone with Internet access. Volunteers also use Wikipedia discussion forums and "Talk pages" to debate the editorial policies and decisions required for reliable and neutral content.

7. Other Projects include Wikimedia Commons, an online repository of free images, sound, and other media files; Wikibooks, a platform for the creation of free textbooks and annotated texts that anyone can edit consistent with the policies of the site; Wikinews, a collaborative journalism platform for volunteers to create and edit original news articles; and Wiktionary, a collaborative project for creating a free lexical database in nearly every language.

C. The Wikimedia Community

8. Wikimedia encourages individuals around the world to contribute to the Projects by communicating information to Wikimedia. Wikimedia receives and maintains this information, and subsequently communicates it to the many other individuals who seek to access, engage with, and further add to Wikimedia's archive of knowledge. The principal way in which Wikimedia communicates with its community is via the Internet.

9. Wikimedia maintains an active and close relationship with the volunteers, contributors, and many other users from around the world who comprise the Wikimedia community. Wikimedia users play a vital role in many of Wikimedia's functions and are active in the Foundation's initiatives, governance, and development of strategy. Wikimedia exists for its user community and depends upon it: users are responsible for the creation of content on the Projects, and users provide the readership base for the Projects. Both the creation of content and

engagement with that content are essential to Wikimedia's mission. In other words, Wikimedia operates interdependently with its user community in pursuit of a shared set of free-knowledge values.

10. This interdependence is reflected in Wikimedia's Board and decision-making structure. Roughly half of the members of Wikimedia's Board of Directors are selected by community members. The Wikimedia Board relies, in turn, on several user-staffed committees to oversee Board elections and recommend new Wikimedia chapters or community organizations. Community members serve on committees responsible for important organizational decisions, such as the Funds Dissemination Committee, which considers grant applications and provides substantive input on Wikimedia's annual plan, and the Language Committee, which proposes and coordinates Wikimedia projects in new languages. Moreover, the Wikimedia community is heavily involved in enforcing Wikimedia's community or project policies, which are largely created by the community. Privacy violations can be reported to an Ombudsman Committee, staffed by volunteers, and a volunteer-staffed Arbitration Committee handles escalated cases related to user conduct and abuse of policies. In sum, Wikimedia routinely makes core organizational decisions only after soliciting input and preferences of its users, including on topics such as its public-policy positions, the creation of new features and Projects, corporate strategy, and budgetary matters.

11. Community members around the world contribute to Wikimedia in other ways as well. The community provides Wikimedia with input on a variety of issues through a number of mailing lists hosted by Wikimedia. In addition, Wikimedia staff frequently engage in "Community Consultations," in which community members can offer their views on strategy, budget, public policy, and other matters directly. Wikimedia also receives significant financial

support from the community in the form of donations; affiliate organizations work with Wikimedia to help develop projects and allow Wikimedia fulfill its mission; and grantees (i.e., recipients of Wikimedia grants) perform important work to advance the Wikimedia movement. Community members are also deeply involved in the development and review of the computer code that supports the Projects.

12. Additionally, as stewards of the Wikimedia Projects and as reflected in Wikimedia's privacy policies, Wikimedia strives to protect the rights of users, including their right to express themselves, and to collaborate together globally, without fear of reprisal. As discussed in greater detail below, Wikimedia undertakes protective measures to ensure the security of its communications and the data it retains. It also resists third-party demands for users' information that are overly broad, unclear, or irrelevant; notifies users individually of information requests when legally permitted; and provides legal defense funds for certain community members who are subject to lawsuits or demands for non-public information as a result of their participation in the Wikimedia Projects.

II. WIKIMEDIA'S INTERNATIONAL INTERNET COMMUNICATIONS

13. "Upstream" surveillance conducted under Section 702 of the FISA Amendments Act ("Section 702") implicates at least three categories of Wikimedia communications: (i) 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; (ii) Wikimedia's internal "log" communications, which help it to monitor, study, and improve the use of the Projects; and (iii) communications of Wikimedia staff.

A. Communications of Wikimedia with Its Community Members

14. As the operator of one of the most-visited websites in the world, Wikimedia engages in an extraordinarily high volume of electronic communications with its users, who read

and contribute to Wikimedia's Projects and webpages, and who use the Projects and webpages to interact with each other. In 2017, Wikimedia sites received over 237 billion "page views," i.e., 237 billion instances of Wikimedia users visiting a particular page on Wikimedia websites, with approximately 74 billion views originating from users in the United States. Over the lifespan of the Wikimedia Projects, Wikimedia's users have edited its pages approximately 3.4 billion times. *See* Bayer Decl. ¶¶ 12, 21 (Exhibit 5). Each of these activities involves Internet communications between Wikimedia and its users—the majority of whom are located abroad.

15. Indeed, as explained in more detail in the Declaration of Tilman Bayer, Wikimedia engages in more than one trillion international communications each year, with individuals who are located in virtually every country on earth. For a user to view, search, log in, edit, or contribute to a Project webpage, the user's device must send at least one HTTP or HTTPS "request" to a Wikimedia server.[2] The number of requests required for a user to access a particular webpage depends on the number of graphics, videos, and other specialized components featured on the page. After receiving such a user request, the Wikimedia server transmits an HTTP or HTTPS "response" to the user's device, in which the content of the requested webpage component is rendered and displayed to the user. Between August 1, 2017 and January 31, 2018, Wikimedia's U.S. servers received approximately 381 billion HTTP or HTTPS requests from users outside of the United States. *See* Bayer Decl. ¶ 27. At this rate, Wikimedia engages in more than one trillion international HTTP or HTTPS communications each year.

[2] "HTTP" and "HTTPS" are common protocols for transmitting data via the Internet, including the content of many webpages. Unlike HTTP, which is unencrypted, "HTTPS" encrypts the connection between Wikimedia servers and the user's browser. *See* Bradner Decl. ¶¶ 120-23 (Exhibit 1).

16. Wikimedia also frequently engages in communications that permit its users to interact with one another more directly. For example, Wikimedia engages in communications that allow users to interact in small or limited groups—including over private and semi-private "wikis" that only certain users, such as user community leaders, can read or edit; private deliberations of user community leaders who help administer the Wikimedia websites; and Wikimedia mailing lists with restricted membership. Community members and leaders often debate and deliberate on organizational policies and decisions in the course of these communications. Separately, Wikimedia also enables registered users to send an email via Wikimedia to another registered user, so long as both have enabled email communications on their Wikimedia accounts. All of these interactions involve communications between Wikimedia and its community members.

17. Wikimedia's communications with its community members are often sensitive and private. Among other things, these Wikimedia communications link each user's page views, searches, and contributions to Wikimedia with his IP address, as well as with other user-specific information. As a rule, Wikimedia maintains as private the IP addresses associated with its community members and their individual interactions with the Projects. The sole exception is when an individual editor reveals his IP address publicly in conjunction with his edits. (Even when editors publicly disclose their IP addresses, many of their exchanges with Wikimedia—such as their page views, searches, and draft contributions—remain private.) *See* Bayer Decl. ¶¶ 12-16.

18. In other words, these communications contain some of the most sensitive information that Wikimedia possesses: which specific webpages each particular person is visiting or editing. They show who is reading—or writing—what. As a consequence, these

communications reveal a detailed picture of the everyday concerns of Wikimedia's users, and often constitute a record of their political, religious, sexual, medical, and expressive interests.

19. At times, these communications also contain questions, comments, or complaints that community members submit to Wikimedia about the performance and operation of its websites. And, at other times, they contain the private deliberations of user-community leaders who help administer the Wikimedia websites and, in that role, discuss Wikimedia's organizational policies and decisions.

20. Finally, Wikimedia's communications with its community members also reveal private information about its operations, including details about its technical infrastructure, its data flows, and its member community writ large.

21. Wikimedia's communications with its community members are essential to its organizational mission, as is its ability to control and maintain the privacy of these communications. Wikimedia's activities depend on its ability to ensure that readers and editors can explore and contribute to the Projects privately when they choose to do so. If these communications were not private, Wikimedia would have immense difficulty both gathering content and sharing information as widely as possible.

22. As a result, Wikimedia takes numerous, costly steps to protect the confidentiality of its communications, including through both legal action and technical measures, some of which are discussed in greater detail below. Wikimedia also assures its community via policies, public statements, and guidelines that it will reject third-party requests for non-public user information unless it is legally required to disclose that information. In keeping with these assurances, Wikimedia resists third-party demands for information that are overly broad, unclear, or irrelevant; notifies users individually of information requests when legally permitted; and

provides legal defense funds for certain community members who are subject to lawsuits or demands for non-public information as a result of their participation in the Projects. These steps are vitally necessary to fostering trust with community members and to encouraging the growth, development, and distribution of free educational content.

B. Wikimedia's Internal "Log" Communications

23. The second category of Wikimedia communications is its proprietary log communications, which it creates and transmits internally as part of its effort to monitor, study, and improve the Projects.

24. Every time Wikimedia receives an HTTP or HTTPS request from a person accessing a Project webpage, it creates a corresponding log entry. Among other private information, logs contain the user's IP address and the URL of the webpage sought by the user. Depending on the location of the user and the routing of her request, the log may be generated by Wikimedia's servers abroad, which in turn send the log to Wikimedia in the United States. Between August 1, 2017 and January 31, 2018, Wikimedia's foreign-based servers transmitted approximately 736 billion log communications to Wikimedia servers in the United States. *See* Bayer Decl. ¶ 27 (quantifying log communications). Wikimedia's proprietary log communications also reveal private information about its operations, including details about its technical infrastructure, its data flows, and its member community writ large.

25. Wikimedia's ability to control and maintain the privacy of its internal log communications is every bit as vital as its ability to ensure the privacy of its communications with community members. The interests described in paragraphs A.17 to A.22 above apply to these internal communications as well. Wikimedia's log communications provide a record of who Wikimedia associates with in the course of its activities, and reveal exactly what information Wikimedia is exchanging with the individuals who contribute to and visit the

Projects. Moreover, Wikimedia creates and transmits these log entries solely for its own internal purposes, as records of its activities, and it does not share them publicly. Because of the sensitivity of this information, Wikimedia seeks to collect and retain as little of it as possible. Indeed, Wikimedia takes steps to protect the confidentiality of these records and the sensitive information they contain—including by keeping them for only a limited amount of time, consistent with the maintenance, understanding, and improvement of the Wikimedia Projects and webpages and with Wikimedia's legal obligations. Still, Wikimedia possesses a large volume of sensitive information about its interactions with its community members, and it transmits a large volume of sensitive information about those interactions every day.

C. Communications of Wikimedia Staff

26. Wikimedia also engages in a third category of sensitive communications. Certain members of Wikimedia's staff routinely engage in sensitive, confidential, and privileged Internet communications with non-U.S. persons located abroad in carrying out Wikimedia's work.

27. Because Wikimedia's activities are global in scope, its staff's international communications are critical to its work. Many members of Wikimedia's U.S.-based staff routinely communicate with individuals abroad using a variety of different modes of electronic communication, including by email (Wikimedia email and Gmail), instant message (Google chat and Internet Relay Chat), video chat (Google Hangout and Skype), public and private "wikis," and an array of electronic third-party work-management tools that facilitate communications (Slack, Google Apps/G Suite, Trello, Sugar, Qualtrics, User Testing, and Salesforce).

28. Wikimedia's international contacts, many of whom are neither U.S. citizens nor permanent residents, include the following:

- Wikimedia's Board of Trustees, seven of whom are located abroad;

- Wikimedia's international contractors, over 140 of whom worked abroad in approximately 45 different countries, including India, Israel, Turkey, Russia, Poland, and Greece, between January 1, 2015 and December 22, 2017;

- Wikimedia's international outside legal counsel, which includes more than 30 law firms from over 20 countries, such as India, Russia, China, Egypt, and Chile;

- project partners and grantees, which encompass a broad spectrum of private-sector, non-profit, and governmental entities, including telecommunication companies, universities, education departments, libraries, and art galleries;

- foreign government contacts, including government officials and political and business leaders; and

- Wikimedia volunteers and other community members.

29. Many of Wikimedia staff's international communications are sensitive, confidential, and legally privileged. Because Wikimedia websites are viewed and edited by hundreds of millions of users all over the world, the organization is routinely confronted with a variety of complex legal issues in various countries. Thus, Wikimedia's U.S.-based attorneys frequently communicate electronically with international outside counsel—based in over 20 countries, including Finland, France, Germany, Greece, Hong Kong, India, Italy, Russia, and the United Kingdom—to discuss privileged matters. As a Wikimedia attorney, I regularly engaged in sensitive, confidential, and legally privileged communications with international outside counsel and Wikimedia contractors located abroad. A few examples of my work in these areas include the following:

- Beginning in 2014 and continuing through May 2017, I regularly communicated via email with Swedish counsel and foreign Wikimedia users in connection with a copyright infringement action involving the Swedish chapter of Wikimedia.

- In 2014 and 2015, I, along with other attorneys in the office, routinely corresponded with Wikimedia's counsel in Finland via email concerning Wikimedia's compliance with Finnish fundraising regulations.

- In 2012 and 2013, I communicated via email with counsel in China. In 2013, these discussions were focused on preparation for the annual Wikimedia conference, known as "Wikimania," which was held in Hong Kong.

- From 2013 through May 2017, I consulted with London counsel via email in connection with a variety of legal issues, including my work revising Wikimedia's internal privacy policies.

30. Wikimedia's U.S.-based legal team also communicates confidentially via the Internet with users abroad who have been threatened, harassed, detained, or sued in connection with their participation in Wikimedia activity, and with users who contact Wikimedia about privacy concerns and other personal matters involving the Wikimedia sites. For instance, I regularly retained and worked with foreign counsel in defending defamation actions involving Wikimedia and individual Wikimedia contributors. In 2014, I engaged counsel in Brazil to help defend against a defamation suit and subpoena seeking the identity of certain Wikimedia users who wished to remain anonymous. From 2012 to May 2017, I worked with Greek counsel to assist in the defense of a defamation action involving an individual Wikimedia user. In both cases, I regularly corresponded via email with users and their counsel.

31. Other members of Wikimedia's U.S.-based staff also engage in sensitive international communications, the confidentiality of which is essential to Wikimedia's work.

32. For example, Wikimedia's grant-making team communicates internationally on a regular basis concerning funding, organizational development, and support for users and volunteer groups who promote the Projects and Wikimedia's mission internationally. Some of these communications contain sensitive information such as personal bank account numbers, scans of photo identification, and private discussions of misconduct or other governance issues among grantees and potential grantees. The grant-making team's international communications also include discussions of volunteers whose work is considered controversial in their home countries—for example, in Venezuela, Iran, Ethiopia, Russia, Belarus, Saudi Arabia, and Kazakhstan. Because the exposure of this information could put volunteers and others in danger, the confidentiality of these communications is critical.

33. Likewise, when Wikimedia conference coordinators plan and promote an annual "Wikimania" conference, referenced above, Wikimedia staff communicate internationally about volunteers' and attendees' real names, email addresses, physical addresses, phone numbers, passport numbers, gender, age, and other affiliations. This information is particularly sensitive when it involves community members from countries of interest to the U.S. government.

III. UPSTREAM SURVEILLANCE OF WIKIMEDIA'S COMMUNICATIONS

34. The Declaration of Scott Bradner explains why it is a virtual certainty that the NSA is copying and reviewing Wikimedia's international communications—i.e., those with Wikimedia's community members, Wikimedia's internal log communications, and communications by Wikimedia staff—in the course of Upstream surveillance.

35. For the following reasons, I believe that it is very likely that Wikimedia is communicating with and about some of the thousands of people and organizations the government has targeted under Upstream surveillance—resulting in the retention of Wikimedia's communications.[3] Wikimedia's communications contain information that plainly falls within the scope of the U.S. government's foreign intelligence interests and its Section 702 collection, specifically.

36. First, Wikimedia routinely communicates with its users and other contacts in geographic areas that are a special focus of the U.S. government's counterterrorism or foreign policy efforts, such as Russia, India, and China. These international contacts have included

[3] At the time the Amended Complaint was filed in June 2015, the NSA used Upstream surveillance to collect communications to, from, and *about* its targets. The NSA reportedly suspended the collection of communications that are merely "about" its targets in April 2017 after violating court-imposed restrictions on Upstream surveillance. *See* Exhibit 45 (Press Release, NSA, *NSA Stops Certain Section 702 "Upstream" Activities*, Apr. 28, 2017, https://www.nsa.gov/news-features/press-room/Article/1618699/nsa-stops-certain-section-702-upstream-activities).

foreign telecommunication companies, such as Orange, Digicel, Airtel, and Beeline; foreign government officials; and hundreds of millions of Wikimedia users located abroad. Since 2011, Wikimedia staff have communicated with, among others, high-ranking leaders of Kuwait and Saudi Arabia; Wikimedia users in conflict zones such as Ukraine; and members of opposition movements throughout the world. Given the nature of Wikimedia's international contacts, and the fact that Wikimedia has hundreds of millions of international contacts, there is a substantial likelihood that at least some of these contacts are targets of Upstream surveillance.

37. Second, many of Wikimedia's international communications contain the kinds of "selectors"—communications accounts, addresses, and identifiers—that the NSA monitors. Hundreds of billions of Wikimedia's international communications (both its HTTP and HTTPS requests and responses, as well as its internal logs of user activity) include details such as website addresses and IP addresses. Furthermore, because Wikipedia is so comprehensive, it has encyclopedic entries for nearly any foreign company, government entity, or terrorist organization that the U.S. government would seek to target. Many of these webpages contain the kinds of selectors that the NSA monitors. For example, website addresses or domain names associated with organizations on the U.S. State Department's Foreign Terrorist Organization List are included on approximately 700 Wikimedia Project webpages—including webpages describing organizations, like Uzbekistan's Islamic Jihad Union, that have been the subject of investigations and prosecutions involving Section 702 surveillance.[4] Additionally, many staff communications contain email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to Wikimedia's work.

[4] *See United States v. Muhtorov*, 187 F. Supp. 3d 1240 (D. Colo. 2015).

38. Third, many of Wikimedia's international communications fall within the Section 702's broad definition of "foreign intelligence information." *See* 50 U.S.C. 1801(e). In addition to the numerous Wikimedia Project pages concerning foreign affairs, Wikimedia staff communicate about issues related to foreign affairs, as the following examples illustrate:

- Wikimedia launched a project called Wikipedia Zero, which was designed to offer Wikipedia free-of-charge on mobile phones in parts of the world where mobile is the primary (or only) means of access to the Internet, and mobile data costs pose a significant barrier to access. To form partnerships with telecommunications companies and to promote Wikipedia Zero, Wikimedia has communicated via email with foreign mobile-phone operators, foreign government officials, and others abroad. These communications include discussions of international law and the policies of foreign companies. Wikimedia has established Wikipedia Zero partnerships with telecommunications companies in more than 70 countries, including Bangladesh, Jordan, Kazakhstan, Pakistan, India, Russia, Saudi Arabia, Tajikistan, and Tunisia.

- Wikimedia is also routinely contacted by, and has been involved in legal action with, foreign government officials and political groups who have expressed dissatisfaction with certain content on Wikipedia pages. For example, in 2015 alone, Wikimedia staff communicated with, among others, government officials and high-ranking leaders of Turkey, Azerbaijan, and Saudi Arabia.

- Wikimedia employees regularly communicate with Wikimedia users from all around the world who are engaged in politically sensitive work or are involved in political opposition movements, including in locations such as Iran, Russia, Egypt, Ukraine, India, China, and Azerbaijan.

- Finally, members of Wikimedia staff also communicate internally about issues of national security and government compliance. For instance, Wikimedia's U.S.-based staff and foreign contractors correspond with one another, and with outside counsel, about the Office of Foreign Asset Control's Specially Designated Nationals List to ensure that Wikimedia's fundraising activities are in compliance with those restrictions.

IV. THE IMPACT OF UPSTREAM SURVEILLANCE ON WIKIMEDIA

39. Upstream surveillance has had a significant and long-lasting impact on Wikimedia's activities and operations.

40. Beginning in June 2013, there were numerous disclosures in the press and by the government concerning Upstream surveillance. The Washington Post and The Guardian were

the first to reveal Upstream surveillance to the public, and the government confirmed the existence of the program shortly thereafter. Over the course of the following year, the government provided additional information about this surveillance to the public.[5] Among the disclosures in the press, the Guardian and others published multiple NSA slides showing that the NSA was surveilling Wikimedia's communications to obtain intelligence information. One of these slides described analysts' ability to learn "nearly everything a typical user does on the Internet" by surveilling HTTP communications—and it identified Wikipedia as a prime example of the HTTP communications collected through NSA surveillance.[6] Another NSA slide published in July 2015 similarly showed that the NSA was intercepting Wikimedia's communications. In particular, it showed that the NSA had designed its search software to allow analysts to identify intercepted Wikimedia communications.[7]

41. These disclosures about Upstream surveillance and the NSA's surveillance of Wikimedia's communications, in particular, caused grave concern and alarm within the Wikimedia community and among Wikimedia staff.

---

[5] *See, e.g.*, Exhibit 15 (Privacy & Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* (July 2014)) (citing numerous official disclosures); Exhibit 17 (Office of the Director of National Intelligence, *DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 702* (Aug. 21, 2013), http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents).

[6] *See* Exhibits 27 & 28 (Glenn Greenwald, *XKeyscore: NSA Tool Collects "Nearly Everything a User Does on the Internet"*, Guardian, July 31, 2013, https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data).

[7] *See* Exhibit 30 (*XKEYSCORE for Counter-CNE*, published in The Intercept on July 1, 2015, https://theintercept.com/document/2015/07/01/xks-counter-cne/ (Slide 9)) (describing computer code that identifies "wikimedia" and "wikipedia" HTTP communications); Exhibit 29 (Morgan Marquis-Boire, *et al.*, *XKEYSCORE: NSA's Google for the World's Private Communications*, Intercept, July 1, 2015, https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications) (publishing the *XKEYSCORE for Counter-CNE* slide deck).

42. As explained below, this surveillance has damaged Wikimedia's ability to carry out its mission by undermining the privacy and anonymity that both Wikimedia and its users depend on. In response, Wikimedia has undertaken a series of protective measures designed to mitigate the threat to its mission and better protect its communications against surveillance.

A. The Impact of Upstream Surveillance on Wikimedia's Users and Consequences for Wikimedia's Work

43. Confidentiality is essential to the work of Wikimedia staff and the organization as a whole. Wikimedia's work depends on the ability to ensure anonymity for individuals who view, edit, or use the Project pages and other Wikimedia websites. The ability to read, research, and write anonymously is essential to free expression and critical to Wikimedia's organizational mission.

44. The "ability of almost anyone to edit (most) articles without registration" is also considered a Founding Principle of Wikipedia. *See* Exhibit 31 (WIKI0008114). This Founding Principle has repeatedly been endorsed in Wikimedia's and the Wikimedia community's public statements. *See, e.g.*, Exhibit 32 (WIKI0006942) ("Privacy on the Internet is closely connected to our mission to disseminate free knowledge. We strive to provide a platform for users from all over the world to exercise their free expression right to share and study educational content. There are circumstances when contributors need to remain anonymous when working on the Wikimedia projects. To that end, the projects allow people to edit under a pseudonym, without providing any personal information, and without even creating an account. We want community members to feel comfortable when working on the projects. And we strongly oppose mass surveillance by any government or entity."); Exhibit 33 (WIKI0008108) ("The Wikimedia projects serve as a platform for people from all over the world to share and study knowledge. Sometimes, people may need to remain anonymous for personal or political reasons when

contributing to the Wikimedia projects. Wikimedia allows people to edit under a pseudonym, without providing any personal information, or without even creating an account. Anonymity and pseudonymity can protect people from retaliation for contributing to the Wikimedia projects."); Exhibit 34 (WIKI0008116) (community policies allow the creation of a second pseudonymous account for privacy purposes, given the importance of anonymity). The importance of anonymity to the Wikimedia community is also articulated in Wikimedia's official policy documents. For example, Wikimedia's Privacy Policy does not require users to create an account to read or contribute to a Wikimedia site, and users are not required to provide a "real name" to verify their identity during account creation. *See* Exhibit 35 (WIKI0006674).

45. Upstream surveillance undermines Wikimedia's ability to conduct its work. Notwithstanding Wikimedia's efforts to protect its information, NSA surveillance, including Upstream surveillance, has resulted and will result in some Wikimedia community members being less willing to engage with the Projects or with Wikimedia staff, because they fear that their communications will be intercepted by the U.S. government and also shared with other governments, intelligence services, and organizations with which the U.S. cooperates.[8]

[8] Users can face government scrutiny, coercion, and other forms of reprisal based on their association with Wikimedia. *See, e.g.*, Joe Sutherland, *2015 Wikipedians of the Year Unveiled in Mexico*, Wikimedia Blog (July 31, 2015), https://blog.wikimedia.org/2015/07/31/wikipedians-of-the-year-2015 (describing the Venezuelan government's revocation of the passport of a Wikimedia user for publishing photos of anti-government protests to Wikimedia). As another example, in March 2013, the Direction Centrale du Renseignement Intérieur ("DCRI"), a French intelligence agency, contacted Wikimedia and demanded removal of an entire Wikipedia article on the ground that it contained classified military information. After Wikimedia was unable to determine what information the DCRI considered classified or high-risk, the DCRI contacted a French Wikipedia volunteer with administrative rights. This volunteer had no role in the creation of the article; however, the DCRI insisted that he use his administrative rights to remove the article immediately, or face serious and immediate reprisals. In the face of these threats, the volunteer removed the article as authorities demanded.

46. For example, following disclosures about the nature and scope of NSA surveillance in the press in the summer of 2013, members of Wikimedia's community expressed fear and concern about Section 702 surveillance, prompting Wikimedia to hold an open "consultation" through an online forum. During this consultation, Wikimedia sought community feedback about the steps it should take to protect the privacy of Wikimedia's activities and its users from Section 702 surveillance. In response, Wikimedia's users from the U.S. and other countries discussed concerns about NSA surveillance activities, including Upstream surveillance. *See* Exhibit 13 (WIKI0008128, -8139) (one user commented on June 15, 2013: "[T]he NSA is also watching all strategic point[s] of internet across the world . . . . certain under sea cable landing have optical splittering [sic] circuits . . . ."). Users expressed their fears not only that their own activities were being surveilled, but also that the community as a whole would see a global drop in participation due to such fears. *See* Alexander Decl. ¶¶ 6, 11 (Exhibit 4).

47. The negative effects of Upstream surveillance on foreign users, described in more detail in the Declaration of James Alexander, are a direct detriment to Wikimedia, its ability to receive and distribute information, its organizational goal of increasing global access to knowledge, and its ability to associate privately with its community for all these purposes. Upstream surveillance also harms Wikimedia's domestic users, whose communications with Wikimedia's foreign servers are subject to this surveillance, and whose ability to exchange information and opinions with Wikimedia's foreign readers and contributors is impaired.

B. Wikimedia's Protective Measures in Response to Upstream Surveillance

48. Due in part to Wikimedia's and Wikimedia users' concerns about U.S. government surveillance, including Upstream surveillance, Wikimedia has undertaken a series of measures to protect its users, communications, and data, including adopting more secure methods of electronic communications, and in some instances self-censoring communications or

forgoing electronic communications altogether. These measures divert Wikimedia's time and monetary resources as a nonprofit entity from other important organizational work.

49. Due in substantial part to Upstream surveillance, Wikimedia transitioned from HTTP to HTTPS as the default protocol for all Wikimedia Project webpages. Historically, the Project websites used HTTP, not HTTPS, by default. However, revelations about Upstream surveillance in the summer of 2013 were a substantial factor in Wikimedia's decision to transition to HTTPS-by-default. As Wikimedia explained on its blog in August 2013, the release of the first NSA PowerPoint slide identifying Wikimedia as subject to U.S. surveillance "prompted our community members to push for the use of HTTPS by default for the Wikimedia projects."[9] On July 31, 2013, Wikipedia founder and Wikimedia Foundation Board of Trustees member Jimmy Wales cited this slide in a post on Twitter, stating that "NSA snooping on what YOU are reading at Wikipedia means I want us to go to SSL [the encryption protocol for HTTPS] sooner." Additionally, in his "State of the Wiki" address in Hong Kong in August 2013, Wales announced that Wikimedia would be transitioning to HTTPS-by-default due to revelations about NSA surveillance in June 2013. I was present for the "State of the Wiki" address and the video recording available at <https://www.youtube.com/watch?v=_w4oCslodDU> appears to be an accurate recording of the speech. Specifically, I recall Wales announcing that Wikimedia would be transitioning to HTTPS-by-default due to the revelations about NSA surveillance.

[9] *See* Exhibit 36 (WIKI0006700) (Ryan Lane, *The future of HTTPS on Wikimedia Projects*, Wikimedia Blog (Aug. 1, 2013), http://blog.wikimedia.org/2013/08/01/future-https-wikimedia-projects/); *see also* Exhibit 37 (WIKI0007108) (Yana Welinder, *et al.*, *Securing access to Wikimedia sites with HTTPS*, Wikimedia Blog (June 12, 2015), http://blog.wikimedia.org/2015/06/12/securing-wikimedia-sites-with-https/).

50. In order to effectively execute its transition to HTTPS-by-default for all Project pages, Wikimedia has devoted four years of full-time employee work allocated across different members of Wikimedia's staff. This transition to HTTPS-by-default has also created additional burdens on specific Wikimedia projects or initiatives. For example, the HTTPS transition necessitated approximately six months of full-time employee work to (1) coordinate with Wikimedia's partners regarding the manner in which the transition would affect the "Wikipedia Zero" project; and (2) provide related technical support.

51. Wikimedia initially had significant reservations regarding how the transition would affect users in large restricted corporate networks or users in countries such as China and Iran, for whom Wikimedia project webpages might or would become inaccessible if they were transitioned to HTTPS. Had it not been for revelations about the NSA's Upstream surveillance, it is likely that Wikimedia would not have transitioned all of its Project webpages to HTTPS-by-default, and instead would have relied on a less burdensome approach through which users could "opt-in" to using HTTPS. Revelations related to Upstream surveillance also contributed to Wikimedia's execution of the transition process on an accelerated basis. *See* Exhibit 38 (WIKI0002298) (statement on May 23, 2014 from Erik Möller, VP of Wikimedia Engineering and Produce Development: "Given increased concern about surveillance/monitoring, and our general commitment to protect user privacy, I expect we'll want to renew our emphasis on encryption and security, including: at least shifting search engine traffic to HTTPS via rel=canonical[;] . . . enabling IPSEC[;] investigating techniques to defeat traffic detection[;] making a definitive decision on whether to force HTTPS for all users.").

52. Due largely to Upstream surveillance, Wikimedia also implemented Internet Protocol Security ("IPsec"). IPsec is a secure network protocol suite that authenticates and

encrypts the packets of data sent over a network. To effectively execute IPsec implementation and maintenance, Wikimedia allocated approximately two years of full-time employee work.

53. Revelations about Upstream surveillance in the summer of 2013 prompted and was the decisive factor in Wikimedia's decision to implement IPsec. Wikimedia had considered implementing IPsec before the revelations, but only acted once it learned the extent of the NSA's surveillance practices as disclosed in June 2013. Knowledge that the NSA's Upstream surveillance involved tapping the Internet backbone made IPsec implementation necessary to protect the confidentiality and security of Wikimedia's communications. Revelations related to Upstream surveillance also contributed to Wikimedia's execution of the transition process on an expedited basis. *See* Exhibit 39 (WIKI0006564, -6566) (statement on July 8, 2013 from Tim Starling, Wikimedia Engineer: "For users geolocated in Europe, HTTPS connections are terminated in esams [Wikimedia's Netherlands server] and then the requests are forwarded unencrypted to eqiad [Wikimedia's U.S. server]. This compromises the security of the system. Recent news articles indicate that the physical security of the internet backbone may not be as good as previously assumed. I propose buying dedicated IPsec hardware for each DC, sufficient to encrypt cache-to-cache traffic and thus protect the privacy of our users.").

54. The transition to HTTPS-by-default and IPsec implementation required a capital expenditure on technical infrastructure:

(i) Wikimedia spent approximately €214,148.46 on Cache/TLS-termination servers located in Amsterdam, Netherlands.

(ii) Wikimedia spent approximately $40,384.56 on Cache/TLS-termination servers located in Virginia, U.S.A.

55. Wikimedia has also hired a full-time Traffic Security Engineer at a base salary of approximately €76,000, who will be responsible for implementing and maintaining technical efforts to protect Wikimedia users' reading and editing habits from mass surveillance—including, specifically, from the NSA's Upstream surveillance. *See* Exhibit 40 (WIKI0002344) (listing engineer's job responsibilities, the first of which is to "[p]rotect our users' reading and editing habits from mass surveillance").

56. Wikimedia's primary motivation in hiring a Traffic Security engineer is to maintain ongoing efforts to protect the confidentiality and security of its Internet communications in response to NSA surveillance practices, including Upstream surveillance. If it were not for Wikimedia's extensive efforts to combat the threat of NSA surveillance, Wikimedia would not have expended the additional resources to hire a new employee for this position.

57. In addition, as discussed in the Declaration of James Alexander, revelations about NSA surveillance, including Upstream surveillance, in the summer of 2013 led to a reluctance on the part of international community members to interact with U.S.-based Wikimedia staff. Fears over NSA surveillance of international Internet communications meant that Wikimedia was required to increasingly rely on in-person communications and encrypted messaging systems when interacting with community members. Due to NSA surveillance, including Upstream surveillance, Wikimedia staff have self-censored their speech and in some instances have forgone electronic communications altogether. *See* Alexander Decl. ¶¶ 13-14.

58. After the summer 2013 revelations about Upstream surveillance, Wikimedia also held internal discussions and community consultations specifically related to NSA surveillance. *See* Exhibit 13 (WIKI0008128) (Wikimedia community consultation on NSA surveillance

disclosures). Due in part to user concerns about Upstream surveillance, Wikimedia expedited the negotiation, drafting, and approval of a new Privacy Policy. *See* Exhibit 41 (WIKI0006602) (Wikimedia blogpost summarizing consultation process). Wikimedia staff responded to community concerns over surveillance—including concerns specifically about the NSA's Upstream surveillance—when drafting these policy changes. I assumed a lead role in developing these new privacy policies, which required extensive consultations and several months' worth of work.

59. Wikimedia is a non-profit organization with limited staff and financial resources. The aforementioned resources that Wikimedia devoted to protect the confidentiality of its communications were made at the expense of other organization initiatives and activities that Wikimedia could have undertaken to further advance its mission.

V. CONCLUSION

60. Freedom of speech, freedom of association, and access to information are core values for Wikimedia. As stewards of the Wikimedia Projects, Wikimedia strives to protect the rights of users, including their right to express themselves, and to collaborate together globally, without fear of reprisal. Many of the topics discussed on Wikimedia pages are controversial or politically sensitive. When Wikimedia's users are afraid to read about or contribute to the collective understanding of those topics, the organization's mission of providing free access to knowledge to all, including Americans, is threatened.

61. The intrinsic value of the Wikimedia Projects lies in both what they are and how they are built. They are an ever-expanding resource of information and ideas, created through open collaboration and dialogue. Upstream surveillance threatens that global collaboration and dialogue, and it does so without deference to the freedoms that ensure free and open access to knowledge for all.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on December 18, 2018 in San Francisco, California.

Michelle Paulson

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

Plaintiff's Exhibit 4

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, *Plaintiff*, v. NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE, *et al.*, *Defendants*.	No. 1:15-cv-00662-TSE

DECLARATION OF JAMES ALEXANDER

I, James Alexander, declare:

1. I am a resident of Daly City, California, over the age of eighteen. I have personal knowledge of the facts stated in this declaration and if called to testify I could and would testify competently thereto. I am providing this declaration in my capacity as a former employee of the Wikimedia Foundation, Inc. ("Wikimedia").

2. I graduated from the University of Rochester in 2010 with a Bachelor of Arts in Economics. I have been a volunteer editor on Wikimedia projects since November 2006 and worked professionally at Wikimedia from August 2010 until December 14, 2018. As an employee at Wikimedia, I worked with Trust and Safety investigations and community management, and in June 2013, I became a full-time Manager for Wikimedia.

3. Beginning in August 2015 until December 14, 2018, I was the Manager for Trust and Safety at Wikimedia. Between June 2013 and August 2015, I was Manager of Wikimedia's Legal and Community Advocacy team. As Manager for Trust and Safety at Wikimedia, I focused on liaising and working with Wikimedia community members who have special administrative responsibilities requiring high levels of trust, including users who have access to private data and

other sensitive information. I also worked on threats of harm to community members or the public that arise in the context of the twelve free-knowledge projects ("Projects") that Wikimedia operates. As Legal and Community Advocacy Manager, I occupied a similar role, coordinating community consultations on new Wikimedia policies and procedures, and acting as primary investigator on threats to community members and other members of the public.

I. Impact of Upstream Surveillance on Wikimedia and its Community Members

4. Since the public first became aware of Upstream surveillance in June 2013, Wikimedia community members have been less willing to read, contribute to, or otherwise engage with Wikimedia Projects and Wikimedia staff online. Due to NSA surveillance, including Upstream surveillance, numerous Wikimedia users around the world have expressed their reluctance to participate in the Wikimedia movement, to read and edit Wikimedia pages, and to share information or communicate with Wikimedia's staff. Wikimedia users have done so in a variety of ways and settings, including but not limited to Wikimedia community forums, Wikimedia discussion groups, and in communications with Wikimedia employees. After the public revelations about Upstream surveillance began in June 2013, Wikimedia staff received numerous complaints about NSA surveillance from users in the United States and around the world. In dozens of these complaints, which occurred in person or through Internet messaging applications, community members either specifically referenced Upstream surveillance by name or the context made clear that they were referring to Upstream surveillance as the basis for their concern.

5. The impact of NSA surveillance—including Upstream surveillance—on Wikimedia community members has taken several forms.

6. Wikimedia staff, myself included, have had numerous conversations with Wikimedia users in the United States and abroad who have self-censored their speech with Wikimedia, or altered or limited their engagement with Wikimedia due to NSA surveillance, including Upstream

surveillance. Many of these individuals are involved in political or social activism and live or work in geopolitical areas that are a special focus of the U.S. government's counterterrorism or foreign policy efforts, such as Iran, Russia, Egypt, Ukraine, India, China, and Azerbaijan. These individuals have engaged in repeated acts of self-censorship vis-à-vis Wikimedia because of NSA surveillance: some refuse to discuss sensitive political topics on which they once spoke candidly; some will now only speak in person rather than over email or other communication channels they used to use; and some will only speak through intermediaries. Users fear NSA surveillance, including Upstream surveillance, and the consequences of that surveillance. In particular, they fear information about their activity on Wikimedia sites could, among other things, identify them, jeopardize or undermine the political or social movements in which they work, or otherwise result in harm to themselves or their families. Many of them were especially concerned about their online activity on Wikimedia project pages because of published NSA slides showing that the NSA was surveilling Wikimedia communications in order to obtain intelligence information. *See* Exhibit 8 (WIKI0006462, -6471-73) (Wikimedia-hosted email list discussing NSA slide with Wikimedia logo).

7. Due in part to concerns about U.S. government surveillance, including Upstream surveillance, some Wikimedia community members abroad have self-censored their speech by refusing to transmit photo identification to Wikimedia staff over the Internet. To gain access to certain tools and access privileges for Wikimedia Projects, community members were historically required to send Wikimedia a copy of their official government-issued identification so that their identities could be confirmed. On several occasions since the public first became aware of Upstream surveillance, users have told Wikimedia that they would not transmit photo identification to Wikimedia via the Internet because of concerns about U.S. government

surveillance. One user stated in a community consultation about Wikimedia's privacy-related policies, "I am . . . very concerned and feel deeply uneasy about (re-)sending a copy of my ID—which is probably one of the most delicate information the WMF can hold—to an organization in a country where countless government agencies can force them to reveal any and all information they want, or even get the information without a court's approval or the subject's awareness. (Yes, I'm looking at the U.S., the recent scandals around the NSA, and the worryingly broad scope of the CIA and other intelligence-gathering organisations.)" *See* Exhibit 9 (WIKI0006410, -6417). These refusals by users to transmit photo identification to Wikimedia due in part to concerns about NSA surveillance have directly affected Wikimedia's ability to carry out its work. They have forced Wikimedia staff to find other, less convenient ways to review community members' identification, including via in-person meetings with international community members.

8. Similarly, due to NSA surveillance, including Upstream surveillance, Wikimedia community members have expressed reluctance to share private data when seeking Wikimedia's assistance in making arrangements to attend Wikimedia conferences or events. Trust and Safety and other teams have also operated through intermediaries when communicating with users in countries of interest to U.S. intelligence agencies, in an effort to avoid surveillance of text-based Internet communications.

9. In addition, certain community-elected users with advanced access to Wikimedia tools and settings, known as "stewards," have avoided email communications with Wikimedia due to NSA surveillance, including Upstream surveillance. Historically, stewards communicated via email regarding a variety of issues arising from Wikimedia's activities, including sensitive conversations about perceived threats to the safety and security of community members. However, after the public first became aware of Upstream surveillance in the summer of 2013, the stewards

expressed reluctance to communicate via email regarding sensitive issues. Thus, in order to work with the stewards on sensitive topics, Wikimedia began to hold regular encrypted videoconference meetings with the stewards.

10. As another example, due to NSA surveillance, Wikimedia community members have sought to use special applications that completely anonymize their communications with Wikimedia. To maintain the integrity of content on Wikipedia, Wikimedia does not permit users with editing privileges to rely on software such as Tor—an Internet browser application that helps anonymize communications online—to shield their IP addresses from Wikimedia. Since the public first became aware of Upstream surveillance in June 2013, Wikimedia community members abroad, including American citizens, have increasingly requested exceptions to this policy as part of efforts to avoid NSA surveillance activities. *See* Exhibit 10 (WIKI0009221, -9222) ("I am a US citizen living abroad. According to recent news reports this places me in a category for elevated surveillance by my government . . . . I prefer to minimize such invasions of my privacy and so use TOR where possible. The global block on TOR exit points has reduced my spontaneous contributions to the WMF projects I am still somewhat involved with."); Exhibit 11 (WIKI0009218, -9219) ("I would like to use Tor while editing Wikimedia wikis, but it seems Wikimedia blocks all Tor exit nodes. . . . I am concerned that [the Philippines] will take hard measures like spying on Filipino citizens and collaborating with the NSA. That's why I am using Tor to prepare if this happens."). I have also had in-person conversations with users who have stated that they would not feel comfortable contributing to or editing Wikimedia pages without using anonymizing software.

11. Wikimedia users have also expressed their concerns about NSA surveillance—and how that surveillance deters users from participating in Wikimedia Projects—through Wikimedia

community forums and similar web pages. Wikimedia hosts a number of forums and other pages in which Wikimedia users converse on a range of topics, including their use of, and participation in, Wikimedia Projects. For example, in December 2013, a group of over 100 users from the German Wikipedia community specifically mentioned NSA surveillance when discussing proposed revisions to Wikimedia policies related to user data. *See* Exhibit 12 (WIKI0001474, -1476) ("The revelations by Edward Snowden and the migration of programs from the Toolserver to Tool Labs prompted discussions among the community on the subject of user data and how to deal with it."). As another example, on a user "Talk page" about the implications of NSA surveillance, one community member stated: "Wikimedia relies on editors being able to edit freely without real world retaliation. This is one reason thinks [*sic*] like no legal threats is a policy. If editors fear retalation [*sic*] by gov for the things they do on Wikimedia, they wont do things that might piss off gov . . . . Obviously we arent at a full surveillance/police state yet, but things like that happen one small step at a time. This is a large step." *See* Exhibit 13 (WIKI0008128, -8144). Indeed, users feared U.S. surveillance of their communications and the potential consequences. Because of NSA surveillance, including Upstream surveillance, many Wikimedia users indicated to me and other Wikimedia staff in conversations in person and through encrypted messaging applications that they feared not only participating in Wikimedia Projects as contributors or editors, but also even reading or visiting Wikimedia pages. They feared NSA surveillance of their communications with Wikimedia and the consequences of that surveillance. In particular, they feared that the information could be used by the U.S. government to reveal users' identities, to identify their political or social activism, or to detect anti-American bias.

12. When users self-censor their speech or otherwise limit their engagement with Wikimedia, it directly harms Wikimedia's ability to carry out its mission to develop and disseminate free

educational content. This disengagement also interferes with the work of Wikimedia staff, discussed in more detail below.

II. Interference with the Work of Wikimedia and its Staff

13. Due to NSA surveillance, including Upstream surveillance, Wikimedia staff have self-censored their speech and in some instances have forgone electronic communications altogether. NSA surveillance, including Upstream surveillance, has made it more difficult for Foundation staff to receive information from and effectively respond to community members—an essential part of running an international community-based organization like Wikimedia. Wikimedia staff have been forced to rely more heavily on in-person meetings and encrypted messaging systems to preserve the confidentiality and security of their communications. As a result, Wikimedia has suffered harm to its institutional goals.

14. Since the public became aware of Upstream surveillance in June 2013, Wikimedia staff on the Trust and Safety team have traveled to attend international Wikimedia conferences more frequently to communicate about sensitive issues in person with community members who are concerned about NSA surveillance, including Upstream surveillance, of their Internet communications. The Trust and Safety team sent at least two additional staff members to each of the annual "Wikimania" conferences held from 2014 through 2018; these conferences are held at locations around the world and the cost of attendance can reach several thousand dollars per staff member. Wikimedia has also sent additional staff each year to attend the "Wikimedia Conference" in Berlin to communicate about sensitive issues in person. Finally, members of the Trust and Safety team have more frequently attended additional country-specific conferences, especially in locations around the world where community members have expressed concerns about NSA surveillance, including Upstream surveillance, such as Germany, Austria, the Middle East, and Eastern Europe. I was personally involved in the decision to send more Wikimedia staff to attend

these events, and the decision was strongly influenced by the fact that Wikimedia community members and affiliate organizations were not comfortable having sensitive conversations online about issues crucial to Wikimedia's mission.

15. Forgoing email and other forms of text-based Internet communications has other adverse consequences on Wikimedia staff. The use of encrypted messaging systems often requires staff to publicly disclose their personal contact information when they otherwise would not have done so. For example, one encrypted messaging system that I frequently used to communicate with community members and other international staff—WhatsApp—requires that I disclose my mobile phone number for account verification. Because Wikimedia lacks the resources to provide staff with mobile phones and data plans, I disclosed my personal mobile phone number to community members in order to use WhatsApp, when I would otherwise not have done so.

16. Due to Upstream surveillance, the Trust and Safety team cannot communicate and operate as effectively worldwide.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on December 17, 2018 in San Francisco, California.



James Alexander

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

Plaintiff's Exhibit 5

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, *Plaintiff*, vs. NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE, *et al*., *Defendants*.	No. 1:15-cv-00662-TSE

DECLARATION OF TILMAN BAYER

I, Tilman Bayer, declare:

1. I am a resident of San Francisco, California, over the age of eighteen. I have personal knowledge of the facts stated in this declaration and if called to testify I could and would testify competently thereto. I am providing this declaration in my capacity as an employee of the Wikimedia Foundation, Inc. ("Wikimedia").

2. I am a Senior Analyst in Wikimedia's Product Analytics team, and have been a full-time employee of the organization since 2012. My responsibilities include the reporting of pageview statistics and other key web traffic metrics to Wikimedia's executives and board. I hold degrees in mathematics from the University of Cambridge (Certificate of Advanced Study in Mathematics) and the University of Bonn (diploma, equivalent to a Master's degree in the US).

3. As explained in further detail in the Declaration of Michelle Paulson (Exhibit 3), Wikimedia is a 501(c)(3) nonprofit organization dedicated to encouraging the growth, development, and distribution of multilingual educational content, and to providing the full content

of these "wiki"-based projects to the public free of charge.[1] Wikimedia operates twelve free-knowledge "Projects" on the Internet, including Wikipedia, a free-access, free content encyclopedia that is the Internet's largest and most popular reference work, and one of the top ten most-visited websites in the world. At the time of the filing of the Amended Complaint in 2015, Wikipedia received more than 400 million visitors each month. *See* Exhibit 44 (WIKI0008271). As of February 2018, the site has grown to contain more than 47 million articles in over 288 languages, and in 2017 it received visits from more than 1 billion unique devices each month.

4. Wikimedia performs a variety of activities that support the Wikimedia movement. Most relevant to my testimony here, Wikimedia provides technical infrastructure for the Projects, and operates over 1000 servers located in the United States, in the Netherlands, and since March 2018, in Singapore. In response to Defendants' written discovery requests in this litigation, I was tasked with quantifying the volume of Internet communications that are transmitted by Wikimedia's servers. My analysis quantified communications by overarching category, Internet protocol, and country of origin. The results of these analyses were produced during discovery. *See* Exhibits 14, 42, and 43. I also quantified and verified other statistics relevant to the volume of Wikimedia's communications, a subset of which are produced herein. *See infra* ¶ 29.

I. TECHNICAL BACKGROUND

A. HTTP/S Requests and Responses

5. A brief description of how computers communicate over the Internet is helpful to understanding the nature of Wikimedia's communications with its users. More fulsome explanations of these technical processes are provided in the expert Declaration of Scott Bradner (Exhibit 1).

[1] A "wiki" is an application that allows collaborative modification, extension, or deletion of its content or structure.

6. The hypertext transfer protocol, or HTTP, is the foundation for data communication over the world wide web and facilitates the exchange of information between computers. HTTP is a "request/response" "Application Layer" protocol that governs how communications occur between "clients" and "servers." A "client" is often a software application, such as a web browser, that initiates a request to connect with a "server," which may be a computer hosting a website. To access a particular webpage, a client must send at least one HTTP request to the relevant server. The number of requests required for an Internet user to access a particular webpage depends on the number of graphics, videos, and other specialized components featured on the page. A server responds to a request by providing the requested "resource." Uniform Resource Locators, or URLs, both identify a resource and describe its location or address. When an Internet user enters a URL address into their web browser using the "http" or "https" web address format, or when a user clicks on a "link" to a webpage, they are actually instructing their web browser (the client) about which resource to request and where to find it.

B. HTTPS and Wikimedia Projects

7. Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP. Web browsers use the URL convention of replacing "http:" with "https:" to indicate that the browser is to communicate with the web server using the "Transport Layer Security" (TLS) protocol instead of the unencrypted protocol used by HTTP. HTTPS operates between the application and transport layers, and encrypts the HTTP application layer communication.

8. Over the past several years, Wikimedia has transitioned to the use of HTTPS by default. *See* Paulson Decl. ¶¶ 49-50. Currently, HTTPS is enabled on all Wikimedia Project websites. If a user requests a Wikimedia site using "http:" in their web browser, they receive a "redirect" response from Wikimedia's servers, which includes the URL information from the user's request.

C. Other Internet Communications Protocols

9. The Transmission Control Protocol (TCP) is a transport layer protocol used to provide a reliable data stream between network nodes. It is used by most major Internet applications including email and the world wide web.

10. The User Datagram Protocol (UDP) is a transport layer protocol that provides a way to send packets from one network node to another network node. Many applications use UDP for transport including some voice and video streaming applications.

11. The Internet Control Message Protocol (ICMP) is a supporting communications protocol used by network devices, including routers, to send operational information, including error messages.

II. WIKIMEDIA PROJECT PAGES AND FEATURES

A. Editing Project Pages

12. All twelve of the Wikimedia Projects are written, edited, and curated collaboratively online by volunteers. Wikimedia users can contribute to Project websites anonymously, under a pseudonym, or under a username that reflects their real identity. As of March 2018, there have been approximately 3.4 billion edits over the lifespan of the Wikimedia Projects.

13. Users can edit a specific Wikimedia Project page via an "Edit" page, which contains a text box with an editable version of the article. An example of an Edit page is depicted in Figure 1 below.

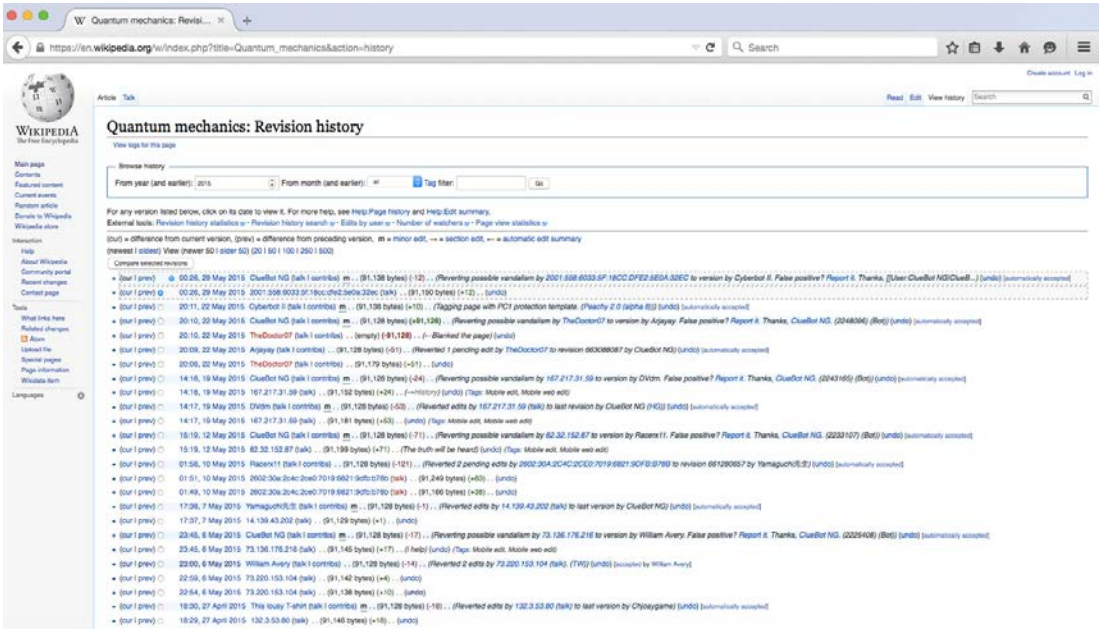
Figure 1



14. Any revisions on this edit page will generally remain private until the user selects the "Publish changes" option (earlier named "Save page" or "submit changes") at the bottom of the screen. If a user selects "show preview" while editing a draft, the changes are communicated between the user's browser and Wikimedia's servers. After the user saves her changes, the user's revisions are publicly visible on the page.

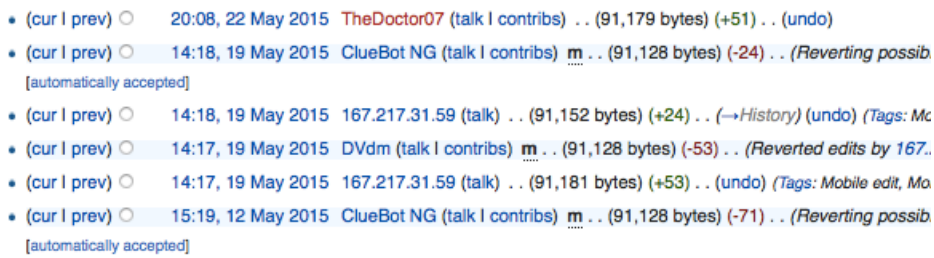
15. The revision history for every page on each of the twelve Projects is publicly visible by clicking on the "View history" or "History" tab on the right side of the screen. This revision history includes unique edits made by individual users. An example of a revision history page is depicted in Figure 2 below.

Figure 2



16. Figure 3 displays a portion of the revision history of the Wikipedia page on "Quantum mechanics." As illustrated in this Figure, when a user who is not logged in as a registered user edits the article, the user's IP address information is visible next to a link to the contributions from that IP address. When a user contributes while logged in to his account, the corresponding revision history page does not reveal the user's IP address. Instead, the revision history page displays the user's username; a link to the user's contributions; and a link to his "User page." That history of the user's contributions and edits is also available via a "Special: Contributions" link from the User page.

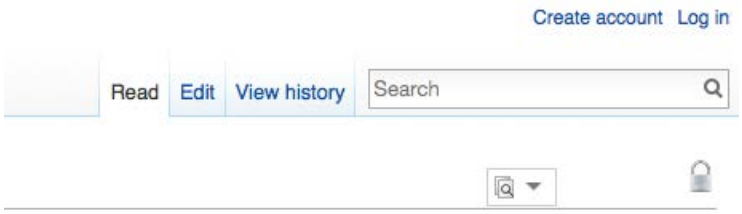
Figure 3



B. Searching and Navigating Wikipedia

17. As shown in Figure 4, users may search Wikipedia by entering a search term; on the desktop version of the site, shown here, the search box is located in the upper-right corner of the screen.

Figure 4



18. Where the search identifies a Wikipedia page with a title that corresponds exactly to the search team, the user is sent directly to that page. The URL of the resulting page incorporates the relevant topic and reveals information about the content of the requested page. For example, when a user employs a search for "substance abuse," the resulting webpage URL is https://en.wikipedia.org/wiki/Substance_abuse.

19. When a search does not identify a Wikipedia page with a title that corresponds exactly to the search team, the user is sent directly to a "Search results" page. The URL of the search results page incorporates the search term employed by that user. For example, if a user searches for "Kansas City Monsoon"—a fictional event with no corresponding Wikipedia page—he would be directed to a Search results page with the following URL: https://en.wikipedia.org/w/index.php?search=Kansas+City+Monsoon&title=Special%3ASearch&go=Go.

20. Additionally, Wikipedia pages include links to other Wikipedia pages on related topics that enable the reader to access those pages directly from the page being viewed. For instance, the Wikipedia page on "Substance abuse" references "anti-social behavior," and includes

a link to the Wikipedia page on this topic, http://en.wikipedia.org/wiki/Anti-social_behaviour.

21. In 2017, Wikimedia sites received over 237 billion page views, with approximately 74 billion views originating from users in the United States.

C. User Discussions

22. Wikimedia also engages in communications that permit its users to interact with one another more directly. Wikimedia Project pages feature "Talk" pages (also known as "Discussion" pages) in which users can publicly discuss potential changes to an article or other Wikimedia Project page. When viewing a Wikimedia Project page on the desktop version of the site, the link to the corresponding Talk page appears on the top left of the screen. A depiction of a Talk page tab and an article Talk page is shown in Figures 5 and 6 below.

Figure 5

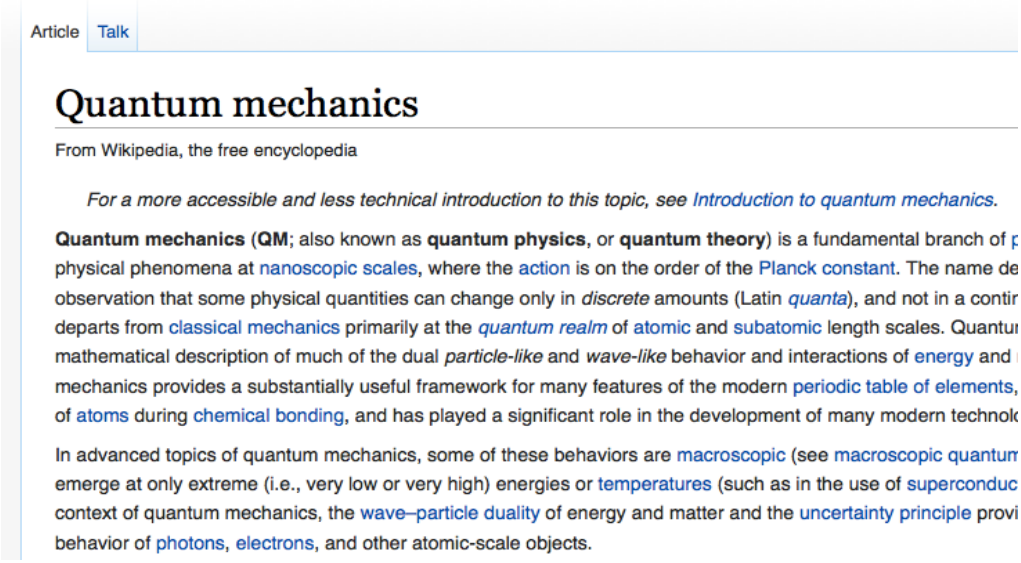
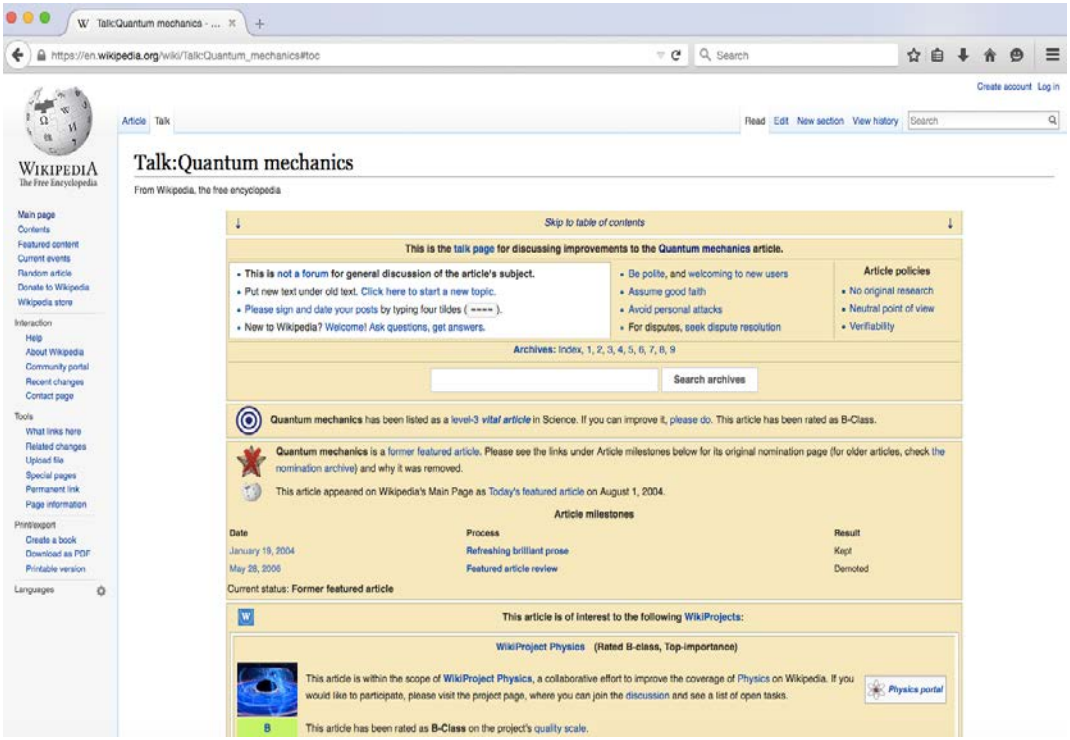
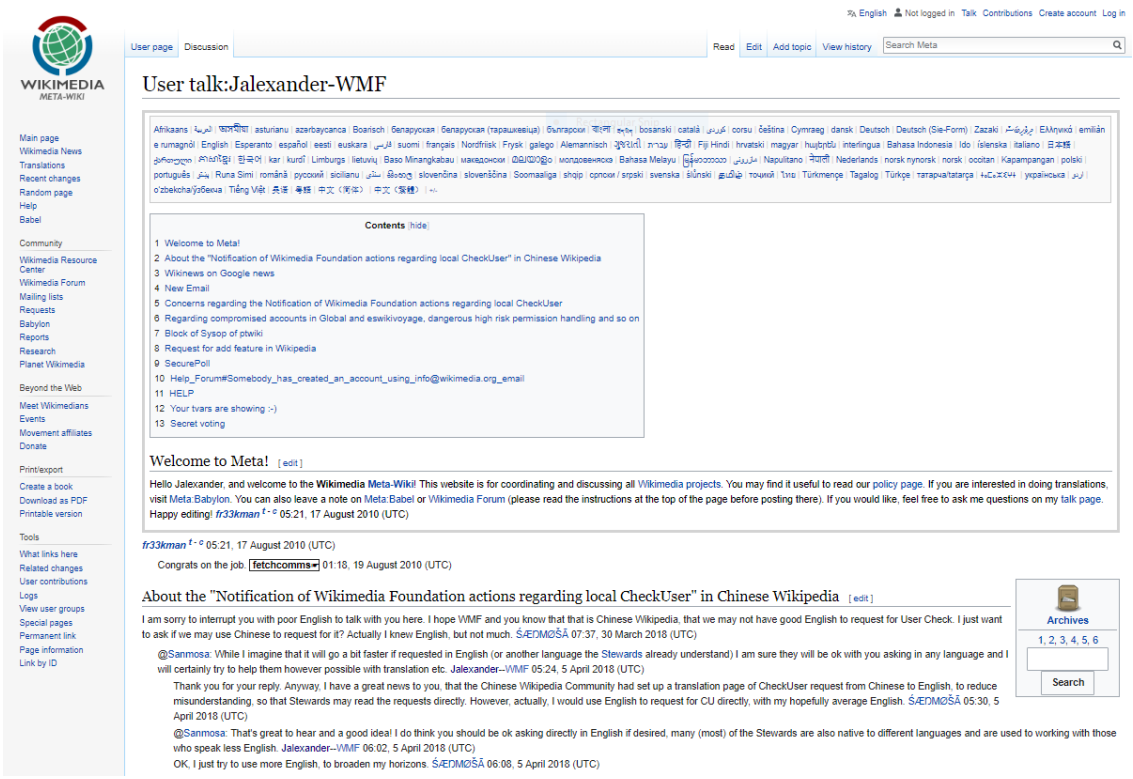


Figure 6



23. User pages also have associated Talk pages. One user may contact another by leaving a message on his Talk page. As with edits, Talk page comments are publicly visible and associated with the commenter's username, or, if the user is commenting without logging in, the user's IP address. Figure 7 illustrates a user's Talk page.

Figure 7



24. Users may also interact with one another and with Wikimedia using private or semi-private communication features on Project websites. The primary examples of these features are discussed below.

- *OTRS*. The Open-source Ticket Request System is a software package employed by Wikimedia since 2004 to address queries, complaints, and comments about the Wikimedia Projects from users. Responses are handled primarily by a group of trusted Wikimedia users who volunteer to answer these queries, complaints, and comments, and certain responses are handled by Wikimedia staff. In other words, OTRS messages are private communications between Wikimedia users or between users and Wikimedia staff.

- *Email User Feature*. This feature allows registered users to exchange emails with one another via Wikimedia, provided that both users have enabled email communications on their Wikimedia accounts. For example, a Wikimedia user can send an email to another Wikimedia user's Gmail account by visiting the intended recipient's User page and selecting an email option. The content of the communication is entered into an HTML form and transferred via HTTPS to Wikimedia servers, and from there to the recipient's email address using the standard SMTP email protocol.

- *Private Mailing Lists.* Users may create or be invited to use "private mailing lists" through Wikimedia. Users must seek permission from the mailing list administrator to receive access to, send, or receive emails through the list, and to read historical archives of mail sent to the list. List messages are sent and received using the SMTP protocol, while archives are accessed via HTTP/S (both via Wikimedia's servers at lists.wikimedia.org). For example, Wikimedia Israel Galleries, Libraries, Archives and Museums coordination is one such private mailing list: https://lists.wikimedia.org/mailman/listinfo/wikimedia-il-glam.

- *Private Wikis.* Some groups of users, for example OTRS volunteers, also employ "private wikis" to communicate about specific topics. These wikis are only accessible by certain users. Wikimedia servers host these communications, which are transmitted via HTTP/S.

III. STATISTICS ON WIKIMEDIA'S INTERNATIONAL INTERNET COMMUNICATIONS

25. As the operator of one of the most-visited websites in the world, Wikimedia engages in an extraordinarily high volume of Internet communications with individual users located around the globe, some of whom are Americans located abroad. *See*, *e.g.*, Exhibit 10 (WIKI0009221, -9222) (American citizen and Wikimedia user located abroad requesting ability to use web application designed to anonymize online activity). Indeed, its servers handle more than one trillion international communications each year, with individuals who are located in every country on earth.

26. Wikimedia's international communications can be divided into the following three categories, each of which contain sensitive and private information related to Wikimedia and its users:

- **Category 1 – *Wikimedia communications with its community members***. Examples of these communications include, but are not limited to, page views to Wikimedia websites, edits and contributions to Wikimedia websites, emails between registered Wikimedia users and emails on Wikimedia's mailing lists. The vast majority of these communications are generated by HTTP and HTTPS requests from users who read and contribute to Wikimedia's Projects, and who use the Projects and webpages to interact with each other.

- **Category 2 – *Wikimedia's internal log communications*.** Wikimedia maintains proprietary "logs" that catalogue a variety of information regarding each HTTP or HTTPS request to a Wikimedia resource. These logs help Wikimedia monitor, study, and improve the Projects. Every time Wikimedia receives an HTTP or HTTPS request from a person

accessing a Project webpage, it creates a corresponding log entry. Depending on the location of the user and the routing of that user's request, the log may be generated by Wikimedia's servers abroad, which in turn send the log entry to Wikimedia in the United States. Wikimedia also uses information about the log communications to inform its site operations, improve user interfaces, and to guide support work for its volunteer community.

- **Category 3 – *Wikimedia's staff communications.*** Wikimedia's office network router located in the United States also handles a variety of border-crossing communications. Examples of these communications include, but are not limited to, Gmail, Google chat, Internet Relay Chat, and Slack. Additionally, Wikimedia staff members use a variety of third-party tools to conduct their work, including, but not limited to, Google Apps/G Suite, Trello, Sugar, Qualtrics, UserTesting and Salesforce. Wikimedia's staff communications reveal a variety of highly sensitive information about Wikimedia's operations, and include communications with international staff who are involved in political or social activism and live or work in geopolitical areas that are a special focus of the U.S. government's counterterrorism or diplomatic efforts.

27. Wikimedia is able to use its server log data to quantify each of these categories of international communications by Internet protocol and country of origin. I led the process of calculating these communications volume figures in response to Defendants' written discovery requests. The results of these analyses are contained in Wikimedia's Exhibit 14 and described below:

Category 1 Volume – *Wikimedia communications with its community members*

- Total HTTP and HTTPS requests from foreign users to Wikimedia's U.S. servers: Between August 1, 2017 and January 31, 2018, Wikimedia's U.S. servers received approximately **381 billion HTTP/S requests** from users outside of the United States. Wikimedia calculated this figure using MaxMind[2] 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.

- Total HTTP and HTTPS requests from U.S. users to Wikimedia's foreign servers: Between August 1, 2017 and January 31, 2018, Wikimedia's foreign-based servers received approximately **2.8 billion HTTP/S requests** from users in the United States. Wikimedia calculated this figure using MaxMind geolocation data to determine the country associated with the client IP of each HTTP/S request transmitted to Wikimedia's servers located outside the United States.

[2] MaxMind is a U.S.-based company that provides widely used databases for Internet geolocation.

Category 2 Volume – *Wikimedia's internal log communications*

- Total log communications transmitted from Wikimedia's foreign servers to Wikimedia's U.S. servers: Between August 1, 2017 and January 31, 2018, Wikimedia's foreign-based servers transmitted approximately **736 billion log communications** to Wikimedia servers in the United States, using the Apache Kafka protocol. These communications were encrypted using IPsec, a secure network protocol suite that authenticates and encrypts the packets of data sent over a network.

Category 3 Volume – *Communications by Wikimedia staff*

- Total logged international TCP connections using Wikimedia's office network or VPN: Between March 1, 2017 and February 28, 2018, Wikimedia's office network router located in the United States logged open Internet connections using the Transmission Control Protocol (TCP) with non-U.S. countries, territories and regions at least approximately **4,948,011** times.

- Total logged international UDP connections using Wikimedia's office network or VPN: Between March 1, 2017 and February 28, 2018, Wikimedia's office network router located in the United States logged open Internet connections using the User Datagram Protocol (UDP) with non-U.S. countries, territories and regions at least approximately **2,207,771** times.

- Total logged international ICMP connections using Wikimedia's office network or VPN: Between March 1, 2017 and February 28, 2018, Wikimedia's office network router located in the United States logged open Internet connections using the Internet Control Message Protocol (ICMP) with non-U.S. countries, territories and regions at least approximately **51,301** times.

28. Wikimedia calculated the Category 3 communications using MaxMind geolocation data to determine the country associated with the source and destination IPs of each of these Internet connections. The router generated a log of all open Internet connections, including their protocol and source and destination IPs, every five minutes, using a program called "conntrack." Connections that remained open for more than five minutes may have been logged more than one time. Connections that remained open for less than five minutes may not been logged at all. These figures include, but are not limited to, connections sent through Wikimedia's virtual private network (VPN), which passed through the same router and can be distinguished in the log by the IP address used to connect.

29. In response to discovery requests in this litigation, I also quantified and verified other statistics relevant to the volume of Wikimedia's communications, a subset of which are contained below in Figure 8.

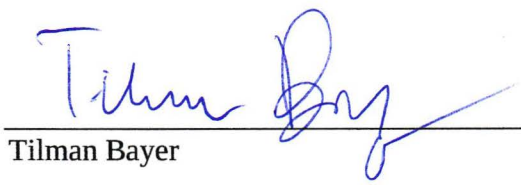
Figure 8

Wikimedia Statistics and Volume Metrics

	Number	Date Range
Wikipedia articles	47,433,067	As of February 9, 2018
Wikipedia languages	288	As of February 9, 2018
Edits over the lifespan of the Wikimedia Projects	approx. 3.4 billion	As of February 28, 2018
Range of monthly unique devices visiting Wikipedia pages	1,521,315,531 (high) / 1,361,541,637 (low)	High/low range for April 2017 to December 2017
Range of monthly U.S. unique devices visiting Wikipedia pages	284,472,345 (high) / 261,065,481 (low)	High/low range for April 2017 to December 2017
Page views	237,586,909,120	January 1, 2017 to December 31, 2017 (one year)
U.S. page views	74,182,143,412	January 1, 2017 to December 31, 2017 (one year)

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on December 19, 2018 in Sindelfingen, Germany.



Tilman Bayer

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

Plaintiff's Exhibit 6

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, *Plaintiff*, v. NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE, *et al.*, *Defendants*.	No. 1:15-cv-00662-TSE

DECLARATION OF EMILY TEMPLE-WOOD

I, Emily Temple-Wood, declare:

1. I am a resident of Downers Grove, Illinois, over the age of eighteen. I have personal knowledge of the facts stated in this declaration, and, if called to testify, I could and would testify competently thereto. I am providing this declaration in my capacity as a Wikimedia Foundation, Inc. ("Wikimedia") community member. I am not an employee or contractor of Wikimedia.

2. I completed a Bachelor of Science degree from Loyola University Chicago, and I am currently a third-year medical student at Chicago College of Osteopathic Medicine at Midwestern University.

I. Background

3. Wikimedia is a nonprofit charitable organization based in San Francisco, California, dedicated to encouraging the growth, development, and distribution of multilingual educational content, and to providing the full content of "wiki"-based projects to the public free of charge.

Wikimedia operates twelve free-knowledge projects ("Projects") on the Internet, including Wikipedia, the world's largest and most popular encyclopedia.

4. I have been a member of the Wikimedia community—as a reader and an editor—for more than 11 years. Since April 2007, I have served as an editor of the English Wikipedia. As an editor, I create original articles for Wikipedia, add original content to existing Wikipedia articles, and edit others' content for accuracy and compliance with Wikipedia's principles, including adherence to a neutral point of view. I have created nearly 400 articles on Wikipedia and have edited thousands more, on topics ranging from biology to women scientists.

5. I have also held several leadership positions within the Wikimedia community. Since November 2007, I have served as an English Wikipedia administrator. Administrators are community leaders, appointed by other community members, who help maintain the integrity of Wikipedia's content. Administrators' responsibilities include blocking certain disruptive users from editing the site, protecting articles from vandalism, deleting and undeleting Wikipedia articles, and mediating disputes.

6. From January 2016 through December 2017, I served on the English Wikipedia's Arbitration Committee. Arbitrators are elected directly by the English Wikipedia community and resolve community disputes over Wikipedia users' conduct when all other dispute-resolution mechanisms have failed. The Committee is also empowered to penalize and ban members who misuse administrative privileges or who are disruptive to the functioning of the community. In addition, the Committee issues binding judgments on matters of Wikipedia policy and clarifies the principles of Wikipedia's governance.

7. Since the summer of 2015, I have served as a Wikipedia Oversighter. Oversighters are appointed after review by the English Wikipedia community and the Arbitration Committee.

Oversighters' responsibilities include removing non-public personal information that is improperly posted to Wikipedia's public webpages, such as phone numbers, addresses, and identities of anonymous users; removing libel and defamatory content; and removing content that infringes copyrights.

II. Relationship Between Wikimedia and Its Users

8. The relationship between Wikimedia and its community of users is so close and intertwined that it is symbiotic: one cannot exist without the other. Users rely on Wikimedia's administrative and technical expertise to create, edit, distribute, and receive free educational content, and Wikimedia relies on its users to create, edit, distribute, and receive that content in furtherance of its mission. Volunteers play critical roles that keep the Projects functioning, such as the administrator, arbitrator, and oversighter roles described above.

9. Wikimedia supports its user community in myriad ways. For one, it operates and provides the technical infrastructure for the Wikimedia Projects, including Wikipedia. It also administers grants to benefit the Wikimedia community and movement, develops software for the community, and works with community members to organize conferences and community-outreach events around the world.

10. Like many other members of the Wikimedia community, I have worked closely with Wikimedia staff. Specifically, my work as an administrator, arbitrator, and oversighter has required extensive communication with Wikimedia staff. In addition, in both 2014 and 2015, I applied for and received grants of $7,000 from Wikimedia to help engage more women as Wikipedia editors. These grants enabled me to develop techniques for recruiting and retaining women editors. Over the course of several years, I also applied for and received scholarships from Wikimedia to attend ten conferences with Wikimedia staff and users.

11. Wikimedia exists to facilitate the user community's work in fulfilling the shared mission of the Wikimedia movement, and the user community would quickly collapse without Wikimedia's infrastructure, network, and support. Wikimedia and its community members depend on one another in pursuit of their shared goal of ensuring that knowledge is free.

III. The Importance of Wikimedia's Non-U.S. Readers and Contributors to U.S. Users

12. My interest in contributing to Wikipedia is based in part on my ability to reach an international audience. Free information is not just for Americans—it is for everyone. Indeed, the very purpose of Wikipedia is to create and distribute the largest and most comprehensive encyclopedia ever written—one of the highest possible quality, that is available for free to every single person on the planet in his or her own language. My contributions to Wikipedia are in furtherance of this mission and of my belief that information on Wikipedia should be freely available to U.S. and non-U.S. persons alike.[1] These contributions have been read by Wikipedia users abroad.

13. I also read and benefit from the contributions of non-U.S. users on a wide array of topics, such as biographies of notable women from around the world, films, history, astronomy, rare diseases, anatomy, and pathology. Wikipedia seeks to amass the sum of human knowledge, and that is simply impossible without the voices of foreign contributors located abroad.

14. Wikimedia community members are spread around the world. As a Wikimedia community member, my relationship with non-U.S. users is crucial to my involvement with Wikimedia.

[1] In this context, by "non-U.S. persons," I mean individuals who are located outside the United States.

15. For example, I interact with and rely on non-U.S. Wikimedia users through the Wikipedia project "Women in Red."[2] This project is designed to address the fact that a disproportionate number of biographies on Wikipedia concern the lives of notable men. Seeking to remedy this gender gap, Women in Red encourages Wikipedia users to create and contribute to articles discussing the biographies and works of notable women. The project has resulted in articles in dozens of languages, including English, Farsi, Catalan, German, Greek, Spanish, French, Italian, Hebrew, Dutch, Albanian, Tamil, Thai, Ukrainian, and Mandarin. As a result of Women in Red, I have read and benefitted from the contributions of many non-U.S. Wikimedia community members to English-language biographies of women.

16. I also deeply value my relationships with the non-U.S. Wikimedia users I have met through Wikimedia conferences. The largest annual conference for the Wikimedia movement, known as "Wikimania," takes place in a new international location each year. The purpose of the conference is to bring together community members from around the world for discussions, trainings, and exchanges of ideas. I have attended four of these conferences, where I have met hundreds of members of the global Wikimedia community.

17. After the conferences, I have continued to communicate with many non-U.S. Wikimedia community members through various means, including Wikipedia "Talk" pages, user "Talk" pages, and private email lists organized by Wikimedia.[3] For example, at the 2013 Wikimania conference in Hong Kong, I had lengthy discussions with my roommate for the week—a Wikipedia contributor from Iraq—about gaps in Wikipedia content. At the conference, I gave a talk about missing women scientists' content, and non-U.S. attendees encouraged me to

[2] *See* https://en.wikipedia.org/wiki/Wikipedia:WikiProject_Women_in_Red.

[3] These pages, also known as "discussion" pages, allow users to publicly discuss potential changes to an article or other Wikimedia Project page.

focus on remedying this gap. After the conference concluded and we returned to our respective countries, we continued these discussions online through Wikipedia pages, which led to the founding of "WikiProject Women Scientists."[4] These conversations inspired me to create and develop dozens of biographies of women scientists on Wikipedia—work that helped deepen my ties to the Wikimedia community, and which led to my being named "Wikimedian of the Year" in 2016.

IV. Importance of Anonymity to Wikimedia Users

18. Anonymity is essential to the Wikimedia user community, including individuals who read or edit Wikimedia Project pages.

19. Although some of my Wikipedia contributions are publicly linked to my real-world identity, I also contribute to Wikipedia under a separate, pseudonymous account when writing about especially sensitive topics. As a medical student, I have a professional interest in gynecology, pediatric gynecology, abortion care, sexually transmitted infections, and LGBTQ health. As a Wikipedia reader, I have accessed Wikipedia pages concerning these issues. As a Wikimedia editor, in order to advance others' understanding of these topics, I have pseudonymously posted images of myself that depict gynecological anatomy and pathology. Given the extremely sensitive nature of these topics, it is essential that I am able to read and contribute to Wikipedia anonymously. When I read and contribute to Wikipedia anonymously, I consider information connecting my identity to the pages I have read or the contributions I have made on Wikipedia to be private.

20. As a Wikipedia user, I am concerned about government surveillance, including Upstream surveillance of my communications with Wikimedia servers located abroad.

[4] *See* https://en.wikipedia.org/wiki/Wikipedia:WikiProject_Women_scientists.

21. Anonymity is critical to non-U.S. Wikimedia users as well. Over the years, I have worked with numerous members of the Wikimedia community who did not disclose their identities because anonymity was so important to them, including Wikipedia administrators, contributors to Women in Red, and users who peer-review articles to ensure that they meet Wikipedia's standards for content quality. Because these users were anonymous, I cannot be certain of their nationality. However, given that some were non-native English speakers, I believe that at least some of these Wikimedia users are non-U.S. persons.

22. Some non-U.S. Wikimedia users have contributed anonymously to Wikimedia about controversial current events in their home countries, because they face grave repercussions if their identities are linked to their online activity. A notable example is an anonymous Wikimedia contributor based in Venezuela. This user posted photographs of anti-government protests in Venezuela to Wikimedia Commons, an online database of media files available for free use. The Venezuelan government eventually uncovered this user's identity and revoked his passport as a result of his contributions to Wikimedia.[5]

23. Upstream surveillance threatens the anonymity and privacy of individuals who visit the Wikimedia Projects. Because of this, and based on my conversations with foreign Wikimedia users living in countries such as Iraq, the United Kingdom, New Zealand, and Singapore, I believe that it is very likely that NSA surveillance has resulted and will result in some foreign readers, editors, contributors, and volunteers being less willing to read, contribute to, or otherwise engage with the Projects, because they fear that their communications will be

[5] Joe Sutherland, *2015 Wikipedians of the Year Unveiled in Mexico*, Wikimedia Blog (July 31, 2015), https://blog.wikimedia.org/2015/07/31/wikipedians-of-the-year-2015/.

intercepted by the U.S. government and also shared with other governments, intelligence services, and organizations with which the U.S. cooperates.

24. In sum, NSA surveillance, including Upstream surveillance, threatens the privacy and anonymity of foreign and domestic members of the Wikimedia community, and that threat discourages individuals from engaging with the Wikimedia Projects.

V. Obstacles to Filing Suit

25. The impact of Upstream surveillance is spread across millions of Wikimedia users and contributors around the world, some of whom may use the Projects a great deal and others who may access the body of knowledge that Wikimedia provides only intermittently. In this context, the obstacles and disincentives that any particular user faces in bringing suit as an individual are significant.

26. First, given the amount of time and resources necessary to pursue a federal lawsuit, as well as the legal and technical complexity of a case challenging the NSA's surveillance practices, I lack the capacity to bring a lawsuit challenging Upstream surveillance on my own behalf. My workload as a medical student would make such a suit impossible. Many Wikimedia community members, including myself, contribute to Wikimedia Projects in their scarce free time, alongside their responsibilities as students, wage-earners, and/or family caretakers.

27. Second, and as importantly, serving as a plaintiff in a lawsuit would threaten the anonymity that users depend on when reading and contributing to the Wikimedia Projects. For example, given the sensitive nature of the articles I read and contribute to on Wikipedia, as summarized above, I would face substantial personal consequences if they were disclosed and dissected in detail in the course of litigation, including through the discovery process.

28. Finally, I fear that if I were to bring a lawsuit challenging U.S. government surveillance, I would risk subjecting myself to unwarranted scrutiny from the U.S. government.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on December 17, 2018 in Downers Grove, Illinois.



Emily Temple-Wood

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

Plaintiff's Exhibit 7

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, *Plaintiff*, v. NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE, *et al.*, *Defendants*.	Hon. T. S. Ellis, III Civil Action No. 15-cv-00662-TSE

DECLARATION OF PATRICK TOOMEY IN SUPPORT OF PLAINTIFF WIKIMEDIA FOUNDATION'S OPPOSITION TO DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

I, Patrick Toomey, a member of the Bar of the State of New York and admitted *pro hac vice* to the Bar of this Court, declare under penalty of perjury as follows:

1. I am an attorney with the American Civil Liberties Union Foundation, and represent Plaintiff Wikimedia Foundation ("Wikimedia") in this matter. I submit this declaration in support of Plaintiff Wikimedia's Opposition to Defendants' Motion for Summary Judgment (ECF No. 161).

2. Filed as Exhibits 1-45 attached to Plaintiff's Opposition to Defendants' Motion for Summary Judgment are true and correct copies of the following documents:

No.	Exhibit
1	Declaration of Scott Bradner and attached Appendix
2	Declaration of Jonathon Penney and attached Appendix
3	Declaration of Michelle Paulson
4	Declaration of James Alexander

5	Declaration of Tilman Bayer
6	Declaration of Emily Temple-Wood
7	Declaration of Patrick Toomey
8	Wikimedia-hosted email list discussing NSA slide with Wikimedia logo, from July to August 2013
9	Wikimedia "Talk page" discussing its non-public information policy, from September to December 2013
10	"OTRS" ticket showing Wikimedia user requesting Tor permissions in September 2013[1]
11	Wikimedia webpage showing Wikimedia user requesting Tor permissions in September 2017
12	Wikimedia document compiling German-user-community appeal concerning privacy in 2013
13	Wikimedia "Talk page" discussing NSA surveillance from June to December 2013
14	Wikimedia Technical Statistics Chart & Supporting Exhibits A-G
15	Privacy & Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* (July 2014)
16	FISC Memorandum Opinion, [*Redacted*], 2011 WL 10945618 (Oct. 3, 2011)
17	Office of the Director of National Intelligence, *DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 702 of FISA* (Aug. 21, 2013), http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents
18	Defendant NSA's Objections and Responses to Plaintiff's First Set of lnterrogatories (Dec. 22, 2017)
19	FISC Submission, *Clarification of National Security Agency's Upstream Collection Pursuant to Section 702 of FISA* (May 2, 2011)
20	Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities, Calendar Year*

[1] This document is a true and correct version of the "OTRS" ticket with certain identifying information redacted, as produced to Defendants in discovery.

	2017 (Apr. 2018), https://www.dni.gov/files/documents/icotr/2018-ASTR----CY2017----FINAL-for-Release-5.4.18.pdf
21	FISC Memorandum Opinion & Order (Apr. 26, 2017)
22	FISC Submission, *Government's Response to the Court's Briefing Order of May 9, 2011* (June 1, 2011)
23	*Big Brother Watch & Others v. United Kingdom*, App. Nos. 58170/13, 62322/14, 24960/15, Eur. Ct. H.R. (2018)
24	NSA Director of Civil Liberties & Privacy Office, *NSA's Implementation of FISA Section 702* (Apr. 16, 2014)
25	*Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (EINSTEIN 2.0)*, 33 Op. O.L.C. 1 (Jan. 9, 2009)
26	Minimization Procedures Used by the NSA in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of FISA (July 2014)
27	Glenn Greenwald, *XKeyscore: NSA Tool Collects "Nearly Everything a User Does on the Internet"*, Guardian, July 31, 2013, https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data
28	NSA slide, excerpted from Exhibit 27 (Greenwald, *XKeyscore: NSA Tool Collects "Nearly Everything a User Does on the Internet"*)
29	Morgan Marquis-Boire, *et al.*, *XKEYSCORE: NSA's Google for the World's Private Communications*, Intercept, July 1, 2015, https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications
30	NSA slide deck, *XKEYSCORE for Counter-CNE*, published in The Intercept on July 1, 2015, https://theintercept.com/document/2015/07/01/xks-counter-cne
31	Wikimedia, *Founding Principles* (accessed Mar. 14, 2018)
32	Yana Welinder, *Opposing Mass Surveillance on the Internet*, Wikimedia Blog (May 9, 2014), https://blog.wikimedia.org/2014/05/09/opposing-mass-surveillance-on-the-internet
33	Wikimedia Public Policy, *Privacy* (accessed Mar. 14, 2018)

34	Wikipedia, *Sock Puppetry* (accessed Mar. 14, 2018)
35	Wikimedia, *Privacy Policy* (accessed Feb. 14, 2018)
36	Ryan Lane, *The Future of HTTPS on Wikimedia Projects*, Wikimedia Blog (Aug. 1, 2013), http://blog.wikimedia.org/2013/08/01/future-https-wikimedia-projects
37	Yana Welinder, *et al.*, *Securing Access to Wikimedia Sites with HTTPS*, Wikimedia Blog (June 12, 2015), http://blog.wikimedia.org/2015/06/12/securing-wikimedia-sites-with-https
38	Wikimedia email describing Tech/Ops goals and the importance of HTTPS (May 23, 2014)
39	Wikimedia document discussing IPsec implementation, including July 8, 2013 statement from a Wikimedia engineer
40	Wikimedia job posting for Traffic Security Engineer (accessed Feb. 8, 2018)
41	Michelle Paulson, *A Proposal for Wikimedia's New Privacy Policy and Data Retention Guidelines*, Wikimedia Blog (Feb. 14, 2014), https://blog.wikimedia.org/2014/02/14/a-proposal-for-wikimedias-new-privacy-policy
42	Wikimedia's Supplemental Exhibit C in response to NSA Interrogatory No. 8 (volume of HTTP border-crossing communications by country)
43	Wikimedia's Supplemental Exhibit D in response to NSA Interrogatory No. 8 (volume of HTTPS border-crossing communications by country)
44	Wikimedia analytics document showing monthly unique visitors to Wikimedia by region, from December 2007 to May 2015
45	Press Release, NSA, *NSA Stops Certain Section 702 "Upstream" Activities*, Apr. 28, 2017, https://www.nsa.gov/news-features/press-room/Article/1618699/nsa-stops-certain-section-702-upstream-activities

* * *

I declare under penalty of perjury that the foregoing is true and correct.

Patrick Toomey

Date: December 18, 2018
New York, New York

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

Plaintiff's Exhibit 8

Re: [Wikimedia-l] NSA [In reply to]

fredbaud at fairpoint

Jul 31, 2013, 6:28 PM
Post #26 of 45 (2064 views)
Permalink

I think it's more reasonable to assume that
> Wikipedia (which shares many features with Google, Yahoo, Twitter, Facebook and other social networks) has been the subject of this kind of demand than that it hasn't. No one with direct knowledge would be able to do anything other than deny it, but we can easily see why data held by Wikipedia (including partially anonymized e-mails, file
> uploads, talk page communication, etc.) would be of interest to
> intelligence agencies.

The capacity of the Wikimedia Foundation to keep a secret of this nature
is low. Simply too many outlaws; something NSA could probably figure out;
they are not called intelligence for nothing.

Fred

Changed "law" to "low"

Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

marc at uberbox

Jul 31, 2013, 6:59 PM
Post #27 of 45 (2051 views)
Permalink

On 07/31/2013 09:27 PM, Ryan Lane wrote:
> I would be fired and jailed before I knowingly let that occur. If this was
> the case I'd very surely not be working for Wikimedia Foundation.

And very many of us live outside the jurisdiction of the entities that would be doing the monitoring and would be very noisy indeed if something of that nature took place.

-- Marc

Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

marc at uberbox

Jul 31, 2013, 7:06 PM
Post #28 of 45 (2050 views)
Permalink

On 07/31/2013 07:52 PM, Nathan wrote:
> If anything, I think it's more reasonable to assume that
> Wikipedia (which shares many features with Google, Yahoo, Twitter,
> Facebook and other social networks) has been the subject of this kind
> of demand than that it hasn't.

You're also making an unwarranted leap there: that the Foundation would
comply with such a demand, if one was made, rather than fight it tooth and nail. In fact, the WMF probably has acquired quite a reputation amongst intelligence circles as being quire uncooperative when it comes
to stomping faces with boots.

There are very few people who work for an organization that has as its primary objective the free dissemination of knowledge that wouldn't be willing to rattle the cages of those who seek to suppress it. If nothing else, we are very good at pointing out egg on faces in a very public, very visible way.

-- Marc

Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

toddmallen at gmail

Jul 31, 2013, 7:11 PM

Also keep in mind that WMF has explicitly stated that they received no such
demand. If they had, they still could say "If we had received such a

Post #29 of 45 (2052 views)
Mailing List Archive
Permalink

demand, we couldn't legally discuss it", still comply with the order, and let us read between the lines. While I don't always agree with WMF, I have
more regard for them than to think they would flat out lie about a matter that important.
On Jul 31, 2013 7:59 PM, "Marc A. Pelletier" <marc@uberbox.org> wrote:

> On 07/31/2013 09:27 PM, Ryan Lane wrote:
> > I would be fired and jailed before I knowingly let that occur. If this
> was
> > the case I'd very surely not be working for Wikimedia Foundation.
>
> And very many of us live outside the jurisdiction of the entities that
> would be doing the monitoring and would be very noisy indeed if
> something of that nature took place.
>
> -- Marc
>
>
> _____
> Wikimedia-l mailing list
> Wikimedia-l@lists.wikimedia.org
> Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
> <mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

_____
Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

jsalsman at gmail

Jul 31, 2013, 7:51 PM
Post #30 of 45 (2056 views)
Permalink

Nathan wrote:
>
>... It seems that most of the data they
> collect is wiped within 3 days; that the data itself can only be
> analyzed under a fairly specific set of minimization rules....

Are you referring to the 2009 Holder minimization rules which per http://m.newyorker.com/online/blogs/closeread/2013/06/how-many-americans-does-the-nsa-spy-on-a-lot-of-them.htmlrequire sharing records on anyone who has ever sent or received email or chat from a foreign national with the FBI, or the more recent "three hop"

minimization rules which require permanent storage of the records pertaining to the roughly one billion people who are connected to people connected to people connected with suspects?

Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

wikimail at inbox

Jul 31, 2013, 9:15 PM
Post #31 of 45 (2051 views)
Permalink

On Wed, Jul 31, 2013 at 9:27 PM, Ryan Lane <rlane@wikimedia.org> wrote:

> I would be fired and jailed before I knowingly let that occur. If this was
> the case I'd very surely not be working for Wikimedia Foundation.
>

Key word there being "knowingly".

Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

tstarling at wikimedia

Jul 31, 2013, 9:44 PM
Post #32 of 45 (2052 views)
Permalink

On 01/08/13 14:15, Anthony wrote:
> On Wed, Jul 31, 2013 at 9:27 PM, Ryan Lane <rlane@wikimedia.org> wrote:
>
>> I would be fired and jailed before I knowingly let that occur. If this was
>> the case I'd very surely not be working for Wikimedia Foundation.
>>
>
> Key word there being "knowingly".

I don't know why the NSA would sneak around in our data centres mirroring our ethernet ports if they already have almost all of our access logs by capturing unencrypted traffic as it passes through XKeyscore nodes.

I think you should save the conspiracy theories until after we switch

anons to HTTPS, that's when they will have an incentive.

-- Tim Starling

Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

akoval at wikimedia

Jul 31, 2013, 10:36 PM
Post #33 of 45 (2051 views)
Permalink

very helpful, james. thanks so much for clue-ing me in. definitely want to know more of the backstory on the chapters sometime. ttyt :)

On Wednesday, July 31, 2013, Tim Starling wrote:

> On 01/08/13 14:15, Anthony wrote:
> > On Wed, Jul 31, 2013 at 9:27 PM, Ryan Lane
<rlane@wikimedia.org<javascript:;>>
> wrote:
> >
> >> I would be fired and jailed before I knowingly let that occur. If this
> was
> >> the case I'd very surely not be working for Wikimedia Foundation.
> >>
> >
> > Key word there being "knowingly".
>
> I don't know why the NSA would sneak around in our data centres
> mirroring our ethernet ports if they already have almost all of our
> access logs by capturing unencrypted traffic as it passes through
> XKeyscore nodes.
>
> I think you should save the conspiracy theories until after we switch
> anons to HTTPS, that's when they will have an incentive.
>
> -- Tim Starling
>
>
> _____
> Wikimedia-l mailing list
> Wikimedia-l@lists.wikimedia.org <javascript:;>
> Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,

--
Anna Koval
Community Advocate
Wikimedia Foundation
415-839-6885 x 6729
akoval@wikimedia.org

Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

akoval at wikimedia

Jul 31, 2013, 10:48 PM
Post #34 of 45 (2060 views)
Permalink

Whoops! :) That wasn't meant to be a reply-to-all. Sorry, everyone.
Rookie
mistake... :]

On Wed, Jul 31, 2013 at 10:36 PM, Anna Koval
<akoval@wikimedia.org> wrote:

> very helpful, james. thanks so much for clue-ing me in. definitely want
> to know more of the backstory on the chapters sometime. ttyt :)
>
>
> On Wednesday, July 31, 2013, Tim Starling wrote:
>
>> On 01/08/13 14:15, Anthony wrote:
>> > On Wed, Jul 31, 2013 at 9:27 PM, Ryan Lane
<rlane@wikimedia.org> wrote:
>> >
>> >> I would be fired and jailed before I knowingly let that occur. If this
>> was
>> >> the case I'd very surely not be working for Wikimedia Foundation.
>> >>
>> >
>> > Key word there being "knowingly".
>> >
>> I don't know why the NSA would sneak around in our data centres

>> mirroring our ethernet ports if they already have almost all of our
>> access logs by capturing unencrypted traffic as it passes through
>> XKeyscore nodes.
>>
>> I think you should save the conspiracy theories until after we switch
>> anons to HTTPS, that's when they will have an incentive.
>>
>> -- Tim Starling
>>
>>
>> _____
>> Wikimedia-l mailing list
>> Wikimedia-l@lists.wikimedia.org
>> Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
>> <mailto:wikimedia-l-request@lists.wikimedia.org?
subject=unsubscribe>
>
>
>
> --
> *Anna Koval*
> Community Advocate
> Wikimedia Foundation
> 415-839-6885 x 6729
> akoval@wikimedia.org
>
>

--
Anna Koval
Community Advocate
Wikimedia Foundation
415-839-6885 x 6729
akoval@wikimedia.org

_____
Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

No, but presenting an appearance of surprise is a bit disingenuous.
P

peter.southwood at telkomsa

Mailing List Archive

Home > Wikipedia Foundation: Page 2 1 2 View All

Post #35 of 45 (2048 views)

Permalink

----- Original Message -----
From: "David Gerard" <dgerard@gmail.com>
To: "Wikimedia Mailing List" <wikimedia-l@lists.wikimedia.org>
Sent: Wednesday, July 31, 2013 11:10 PM
Subject: Re: [Wikimedia-l] NSA

> On 31 July 2013 21:47, Ryan Lane <rlane@wikimedia.org> wrote:
>
>> Why would we expect that we weren't being targeted? Knowing what people
>> are
>> looking up is powerful knowledge.
>
>
> That doesn't make it one dot less reprehensible.
>
>
> - d.
>
> _____
> Wikimedia-l mailing list
> Wikimedia-l@lists.wikimedia.org
> Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
> <mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

_____
Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

peter.southwood at telkomsa

Jul 31, 2013, 11:14 PM

Post #36 of 45 (2047 views)

Permalink

And "non-western" countries probably go further if their technological capacity allows it. If you are not being spied on by "somebody" it is because no-one could be bothered or they havent got around to it yet, not
because any law protects your privacy.
P
----- Original Message -----
From: "Nathan" <nawrich@gmail.com>
To: "Wikimedia Mailing List" <wikimedia-l@lists.wikimedia.org>

> On Wed, Jul 31, 2013 at 5:53 PM, Matthew Walker
<mwalker@wikimedia.org>
> wrote:
>>>
>>> What surprises me is that anyone is surprised by any of this
>>> information.
>>
>>
>> It's one thing to have suspicions and theories about it; but if the third
>> party is constantly denying the allegations and with no recourse
there's
>> no
>> point in getting angry. Now that we have reasonable doubt, I hesitate
to
>> call it proof, we can start making tremendous amounts of noise.
>>
>> ~Matt Walker
>
> I think that's just naive. Of course it was always denied until it
> became impossible to deny it. That's how these things work. But I
have
> honestly assumed for many years that virtually everything transmitted
> over almost any electronic medium was collected and analyzed in
some
> way. That appears to be the case, and in fact, I expected them to
have
> gone further than they have. It seems that most of the data they
> collect is wiped within 3 days; that the data itself can only be
> analyzed under a fairly specific set of minimization rules after the
> approval of a senior executive in the administration, that the rules
> are drawn from generally accepted 4th amendment jurisprudence, etc.
>
> The cynic in me is also convinced that virtually all Western countries
> do the same sort of thing, if probably on a smaller scale. I would bet
> all the money I have that at a minimum the French, the English and
the
> Germans maintain roughly similar intelligence gathering programs.
But
> of course, they will deny it until it becomes impossible to deny it.
>
> _____

> Wikimedia-l mailing list
> Wikimedia-l@lists.wikimedia.org
> Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
> <mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

peter.southwood at telkomsa

Jul 31, 2013, 11:28 PM
Post #37 of 45 (2045 views)
Permalink

Does the law actually require them to lie about data demands when questioned?
P
----- Original Message -----
From: "Nathan" <nawrich@gmail.com>
To: "Wikimedia Mailing List" <wikimedia-l@lists.wikimedia.org>
Sent: Thursday, August 01, 2013 1:52 AM
Subject: Re: [Wikimedia-l] NSA

> On Wed, Jul 31, 2013 at 7:11 PM, Michael Snow
<wikipedia@frontier.com>
> wrote:
>> On 7/31/2013 3:31 PM, Nathan wrote:
>>>
>>> And another thought - you know what unites most of the other
companies
>>> represented by the logos in that image? Leaks have confirmed that
most
>>> of them are the subject of secret orders to turn over huge amounts
of
>>> raw data to the government. They are all bound to secrecy by law,
so
>>> without permission none of them are permitted to describe or
disclose
>>> the nature or extent of the data demands the U.S. government has
made.
>>>
>>> Now if you imagine the puzzle globe on that slide implies that
>>> Wikipedia traffic is retained for intelligence analysis, it's a short

>>> hop to assume that the Wikimedia Foundation is also the subject of a
>>> blanket order transferring its server logs to the NSA.
>>
>> Facebook, Google, Yahoo, and Twitter, yes. But mail.ru? The shift from
>> "most" to "all" in the first paragraph may make it easy to assume the
>> similarity is universal, but it's ignoring the full context. That kind of
>> rhetorical shift is a favorite trick of conspiracy theorists, it's how
>> they
>> get you to make those short hops to unwarranted conclusions.
>>
>> --Michael Snow
>>
>>
>
> It's hardly a conspiracy theory. Given the differences between mail.ru
> and Wikipedia, I should think it would be clear why one might be
> subject to a direct demand for transferring data while the other is
> not. If anything, I think it's more reasonable to assume that
> Wikipedia (which shares many features with Google, Yahoo, Twitter,
> Facebook and other social networks) has been the subject of this kind
> of demand than that it hasn't. No one with direct knowledge would be
> able to do anything other than deny it, but we can easily see why data
> held by Wikipedia (including partially anonymized e-mails, file
> uploads, talk page communication, etc.) would be of interest to
> intelligence agencies.
>
> _____
> Wikimedia-l mailing list
> Wikimedia-l@lists.wikimedia.org
> Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
> <mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

_____
Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

peter.southwood at telkomsa
Mailing List Archive

Thanks, This answers my question.
P

Post #38 of 45 (2047 views)
Permalink

----- Original Message -----
From: "Luis Villa" <lvilla@wikimedia.org>
To: "Wikimedia Mailing List" <wikimedia-l@lists.wikimedia.org>
Sent: Thursday, August 01, 2013 2:13 AM
Subject: Re: [Wikimedia-l] NSA

> On Wed, Jul 31, 2013 at 4:11 PM, Michael Snow
> <wikipedia@frontier.com>wrote:
>
>>
>>> Now if you imagine the puzzle globe on that slide implies that
>>> Wikipedia traffic is retained for intelligence analysis, it's a short
>>> hop to assume that the Wikimedia Foundation is also the subject of
a
>>> blanket order transferring its server logs to the NSA.
>>>
>> Facebook, Google, Yahoo, and Twitter, yes. But mail.ru? The shift
from
>> "most" to "all" in the first paragraph may make it easy to assume the
>> similarity is universal, but it's ignoring the full context. That kind of
>> rhetorical shift is a favorite trick of conspiracy theorists, it's how
>> they
>> get you to make those short hops to unwarranted conclusions.
>
>
> Thanks for the voice of reason, Michael.
>
> As a quick reminder here, before any conspiracy theories about
orders and
> data retention get out of control:
>
> 1) We've flat-out denied any sort of involvement in this, and we
continue
> to stand by that denial:
> https://blog.wikimedia.org/2013/06/14/prism-surveillance-wikimedia/
>
> 2) Take with a grain of salt, of course, but our understanding (based
on
> the few gag orders that have been made public) is that we could be
forced
> to not confirm having received a National Security Letter, but we can't
> actually be forced to lie about it. In other words, if we'd received one

HIGHLY PROTECTED — ATTORNEYS' EYES ONLY FOIA Confidential Treatment Request
WIKI0006473

> we
> would not be allowed to say "we've received one", but we also could not be
> forced to deny it - we'd always have the option to remain silent instead.
>
> 3) We understand that the rules cause some people not to trust our denial,
> and can't entirely blame them! That is why we've asked the government to
> change the rules, so that you can have more trust in us next time we issue
> the same denial:
> https://blog.wikimedia.org/2013/07/18/wikimedia-foundation-letter-transparency-nsa-prism/
>
> This is not to say that the http/https issue isn't important; like
> Engineering, we think progress on that issue is important. But it is
> important to keep "we don't yet deploy https as widely as we'd like"
> separate from "there are secret orders to transfer all our logs to the
> NSA."
>
> Thanks-
> Luis
>
> --
> Luis Villa
> Deputy General Counsel
> Wikimedia Foundation
> 415.839.6885 ext. 6810
>
> NOTICE: *This message may be confidential or legally privileged. If you
> have received it by accident, please delete it and let us know about the
> mistake. As an attorney for the Wikimedia Foundation, for legal/ethical
> reasons I cannot give legal advice to, or serve as a lawyer for, community
> members, volunteers, or staff members in their personal capacity.*
> _____
> Wikimedia-l mailing list
> Wikimedia-l@lists.wikimedia.org
> Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
> <mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

rupert.thurner at gmail

Jul 31, 2013, 11:57 PM
Post #39 of 45 (2057 views)
Permalink

On Thu, Aug 1, 2013 at 6:44 AM, Tim Starling
<tstarling@wikimedia.org> wrote:
> On 01/08/13 14:15, Anthony wrote:
>> On Wed, Jul 31, 2013 at 9:27 PM, Ryan Lane
<rlane@wikimedia.org> wrote:
>>
>>> I would be fired and jailed before I knowingly let that occur. If this
was
>>> the case I'd very surely not be working for Wikimedia Foundation.
>>>
>>
>> Key word there being "knowingly".
>
> I don't know why the NSA would sneak around in our data centres
> mirroring our ethernet ports if they already have almost all of our
> access logs by capturing unencrypted traffic as it passes through
> XKeyscore nodes.
>
> I think you should save the conspiracy theories until after we switch
> anons to HTTPS, that's when they will have an incentive.

tim, and ryan, that is not 100% true. since at least 2010 we know from articles like these:
* http://www.wired.com/threatlevel/2010/03/packet-forensics/
* https://www.eff.org/deeplinks/2010/03/researchers-reveal-likelihood-governments-fake-ssl
that man-in-the middle attacks are possible with and without HTTPS at XKeyscore nodes. the basic problem is, that wikipedia contents is stored in the U.S., and the site is using certificates issued in the U.S. the same country and legislation the NSA is located. this means the certificates can be compromised and users would not (easily) notice it.

the best sign against snooping internet traffic would be if wikipedia will change the hosting to a different country, and use a different

countries ssl certificate. you can bet, that the perceived impact on the U.S. business will be so huge that this intolerable practice will stop, at source, at NSA.

btw, ryan, you talked about firing and jailing - if you did not know that or if you knew it and ignored it, you should be fired or not work at WMF ;) it is _you_ who need to warn about the location beeing vulnerable, and it is _you_ who decide to use vulnerable digicert certificates. but you of course will not be jailed - this seems to happen to people revealing that xkeyscore exists ...

rupert.

Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

rarohde at gmail

Aug 1, 2013, 2:31 AM
Post #40 of 45 (2043 views)
Permalink

On Wed, Jul 31, 2013 at 5:13 PM, Luis Villa <lvilla@wikimedia.org> wrote:
> As a quick reminder here, before any conspiracy theories about orders and
> data retention get out of control:
>
> 1) We've flat-out denied any sort of involvement in this, and we continue
> to stand by that denial:
> https://blog.wikimedia.org/2013/06/14/prism-surveillance-wikimedia/
>
> 2) Take with a grain of salt, of course, but our understanding (based on
> the few gag orders that have been made public) is that we could be forced
> to not confirm having received a National Security Letter, but we can't
> actually be forced to lie about it. In other words, if we'd received one we
> would not be allowed to say "we've received one", but we also could not be
> forced to deny it - we'd always have the option to remain silent instead.
<snip>

If we are going to chase crazy down the rabbit hole, then it may be worth noticing that the NSL gag order makes it a crime to discuss NSL demands with anyone except A) personal legal counsel, and B) persons who are directly necessary to fulfill the demand. In particular, if I (as an individual) am served with an NSL then there is no provision allowing me to tell my boss or my subordinates unless I directly need their help to satisfy the request. If someone with root access were directly served with an NSL, it isn't obvious that WMF executives would ever learn about it. This is one of the ways that NSL gag orders are ridiculous.

-Robert Rohde

Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

george.herbert at gmail

Aug 1, 2013, 2:56 AM
Post #41 of 45 (2056 views)
Permalink

The letters must be sent to the organization rather than an individual. The idea of going to an individual employee and strongarming them may happen, but the law around NSLs is specific.

The court cases to date indicate that if an individual employee got a US NSL and sued over it, the judge would likely take actions that would end the FBI agents careers.

Such individual strongarming would almost certainly use threats or MICE (money, ideology, compromise, ego) enticements and no paper trail to have to testify over in court later.

George William Herbert
Sent from my iPhone

On Aug 1, 2013, at 2:31 AM, Robert Rohde <rarohde@gmail.com> wrote:

> On Wed, Jul 31, 2013 at 5:13 PM, Luis Villa <lvilla@wikimedia.org> wrote:
>> As a quick reminder here, before any conspiracy theories about orders and
>> data retention get out of control:

>>
>> 1) We've flat-out denied any sort of involvement in this, and we continue
>> to stand by that denial:
>> https://blog.wikimedia.org/2013/06/14/prism-surveillance-wikimedia/
>>
>> 2) Take with a grain of salt, of course, but our understanding (based on
>> the few gag orders that have been made public) is that we could be forced
>> to not confirm having received a National Security Letter, but we can't
>> actually be forced to lie about it. In other words, if we'd received one we
>> would not be allowed to say "we've received one", but we also could not be
>> forced to deny it - we'd always have the option to remain silent instead.
> <snip>
>
> If we are going to chase crazy down the rabbit hole, then it may be
> worth noticing that the NSL gag order makes it a crime to discuss NSL
> demands with anyone except A) personal legal counsel, and B) persons
> who are directly necessary to fulfill the demand. In particular, if I
> (as an individual) am served with an NSL then there is no provision
> allowing me to tell my boss or my subordinates unless I directly need
> their help to satisfy the request. If someone with root access were
> directly served with an NSL, it isn't obvious that WMF executives
> would ever learn about it. This is one of the ways that NSL gag
> orders are ridiculous.
>
> -Robert Rohde
>
> _____
> Wikimedia-l mailing list
> Wikimedia-l@lists.wikimedia.org
> Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

_____
Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

Mailing List Archive

Home > Wikimedia > Foundation > Page 2 1 2 View All

emijrp at gmail

Aug 1, 2013, 3:02 AM
Post #42 of 45 (2049 views)
Permalink

It is funny (but also sad) to see how people thought that Internet privacy was respected in Western world. Almost 99% only worried about China/Iran
Internet monitoring and censorship but we had here the most comprehensive
spy system logging every site you read.

Wake up!

Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

wikimail at inbox

Aug 1, 2013, 4:39 AM
Post #43 of 45 (2041 views)
Permalink

On Thu, Aug 1, 2013 at 12:44 AM, Tim Starling
<tstarling@wikimedia.org>wrote:

> On 01/08/13 14:15, Anthony wrote:
> > On Wed, Jul 31, 2013 at 9:27 PM, Ryan Lane
<rlane@wikimedia.org> wrote:
> >
> >> I would be fired and jailed before I knowingly let that occur. If this
> was
> >> the case I'd very surely not be working for Wikimedia Foundation.
> >>
> >
> > Key word there being "knowingly".
>
> I don't know why the NSA would sneak around in our data centres
> mirroring our ethernet ports if they already have almost all of our
> access logs by capturing unencrypted traffic as it passes through
> XKeyscore nodes.
>

Especially not when they can get someone else to do it for them.

I think you should save the conspiracy theories until after we switch
> anons to HTTPS, that's when they will have an incentive.
>

And I thought Ryan Lane was talking about the future, not the past. I certainly was.

Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

rlane at wikimedia

Aug 1, 2013, 10:20 AM
Post #44 of 45 (2044 views)
Permalink

On Thursday, August 1, 2013, Anthony wrote:

> On Thu, Aug 1, 2013 at 12:44 AM, Tim Starling
<tstarling@wikimedia.org<javascript:;>
> >wrote:
>
> > On 01/08/13 14:15, Anthony wrote:
> > > On Wed, Jul 31, 2013 at 9:27 PM, Ryan Lane
<rlane@wikimedia.org<javascript:;>>
> wrote:
> > >
> > >> I would be fired and jailed before I knowingly let that occur. If this
> > was
> > >> the case I'd very surely not be working for Wikimedia
Foundation.
> > >>
> > >
> > > Key word there being "knowingly".
> >
> > I don't know why the NSA would sneak around in our data centres
> > mirroring our ethernet ports if they already have almost all of our
> > access logs by capturing unencrypted traffic as it passes through
> > XKeyscore nodes.
> >
>
> Especially not when they can get someone else to do it for them.
>
> I think you should save the conspiracy theories until after we switch
> > anons to HTTPS, that's when they will have an incentive.
> >
>
> And I thought Ryan Lane was talking about the future, not the past. I
> certainly was.

I'm talking about both.

- Ryan

Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

z at mzmcbride

Aug 12, 2013, 6:05 PM
Post #45 of 45 (1975 views)
Permalink

Anthony wrote:
>And I thought Ryan Lane was talking about the future, not the past. I >certainly was.

I think we should focus on the present, personally.

If a user goes to <https://wikipedia.org>, they're quietly redirected to <http://www.wikipedia.org>. This is true of a large number of domains (e.g., <https://wikimedia.org> and <https://mediawiki.org>).

This has been known about since at least October 2011 (cf. <https://bugzilla.wikimedia.org/31369>) and everyone seems to agree that
it's a pretty evil bug (a user knowingly tries to access a site over HTTPS and is unknowingly routed to HTTP). And yet it's August 2013 and the best
response we seem to have come up with is "install a client-side browser plugin" and "we're working on it."

It's difficult to believe that the Wikimedia Foundation is committed to user privacy when bugs like this go unresolved after so many months. This
bug will celebrate its second birthday in less than two months.

MZMcBride

Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

©2018 GT.net. A Gossamer Threads company.
5th Floor, 455 Granville St., Vancouver, BC V6C 1T1, Canada | Legal

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

Plaintiff's Exhibit 9

USCA4 Appeal: 20-1191 Doc: 18-3 Filed: 07/01/2020 Pg: 528 of 574

Talk:Access to nonpublic information policy/Archives/2013

< Talk:Access to nonpublic information policy

Please do not post any new comments on this page. *This is a discussion archive first created on December 9th 2013, although the comments contained were likely posted before and after this date. See current discussion or the archives index.*

Internal policy on ID collection

This was posted by Geoff on the Privacy Policy talk page but I think would be interesting to those here as well.

> **Wikimedia Foundation - Internal Policy**
>
> **Purpose**
>
> The Wikimedia Foundation ("WMF") may sometimes need to collect copies of identification documents ("IDs") from community members pursuant to established policies of WMF or the community. Examples where community members may need to identify themselves include the following:

Contents

- **Internal policy on ID collection**
  - Wikimedia Foundation - Internal Policy
    - Purpose
    - Collection, Storage, and Access
    - Destruction
  - Illustrations
- **Who's we?**
- **Wikipedia Day 2014**
- **Protect your access**
- **Why should copies of the photos ID be retained ?**
- **CheckUser policy**
- **Data retention forced by what law?**
- **Re-identification and retention of data vs. the NSA**
  - Explain data retention in the policy itself
  - Who needs to identify at all now?
    - Enwiki ACC
  - WMF?
- **Identification**
- **Change of identity information**
- **Valid for Supportteam-members with access to OTRS-queues?**
- **Why a 3-year post removal retention period?**
- **sharing info to someone with an nda**
- **Some food for thought**
- **Purpose**
- **Purpose of retention for address**
- **What about stolen accounts?**
- **Board of Trustees**
- **exact scans vs. data**
  - Draft confidentiality agreement
- **OTRS volunteers**
  - Balancing WMF's need to protect itself with volunteers' need to protect themselves
- **Signing the pledge and resulting liability implications**
- **Consideration of feedback given over the past week**
- **Affected users who will resign if the policy is implemented in its current shape**
- **Volunteer developers**
- **Policy should be rejected!**
- **Attempt at a better evaluation of this draft**
  - Policy itself
  - Title
  - User-friendly summary
  - Purpose paragraph 1
  - Purpose paragraph 2
  - Scope paragraph 1
  - Scope paragraph 2
  - Requirements intro paragraph

- Candidates

Requirements sub-point A
Requirements sub-point B
Requirements sub-point C
Requirements sub-point D part I
Requirements sub-point D part II
Submitting new materials
Submission methods
Submission timeline
Use and disclosure intro paragraph
Use and disclosure sub-point A
Use and disclosure sub-point B
Penultimate paragraph
Final paragraph

Notifications

feedback from otrs agent

disagree with preservation of digital version of id papers
disagree with disclosure of agent private information to community members not bound to the non public information policy
ask for mandatorily notification of non public information disclosure about agent from WMF to concerned agent
Comments

Illegal

Statement from user:aschmidt

Stuff to think about

WMF board, FDC, etc.

Pedantic lawyerly point about use of "age of majority"

Community Committees

(http://meta.wikimedia.org/wiki/Board_elections/2011/en#Prerequisites_to_candidacy) for the WMF Board of Trustees

- Candidates (http://meta.wikimedia.org/wiki/Funds_Dissemination_Committee/Framework_for_the_Creation_and_Initial_Operation_of_the_FDC#Membership) for the Funds Dissemination Committee
- Recipients of WMF grants
- Representatives and agents of user groups and thematic organizations
- Community members (http://wikimediafoundation.org/wiki/Access_to_nonpublic_data_policy) with access to nonpublic user data information [GRB Note: we are currently not keeping such IDs on file.]

This internal policy summarizes the approach to be taken by WMF employees and contractors when handling and storing such community member IDs. The required ID depends on the criteria of the particular policy or practice, but may include copies of passports, driver's licenses, and other government-issued documents showing real name and age.

Collection, Storage, and Access

Copies of IDs provided to WMF by community members will be kept confidential, consistent with any applicable requirements of the WMF privacy policy (http://wikimediafoundation.org/wiki/Privacy_policy). Physical copies of IDs will be kept in locked cabinets designated for this purpose. Electronic copies of IDs will be protected by passwords or other electronic protections in files designated for this purpose.

Access to IDs will be limited to a "need to know" protocol determined by the program administrator. Usually that means only the principal administrators of a program will have access to those IDs. WMF will not share the IDs with outside third parties, unless required by law, covered by a non-disclosure agreement approved by Legal, or necessary to protect the rights, property, or safety of WMF and its employees and contractors.

Destruction

IDs will be kept as long as necessary to satisfy the need of the applicable policy and practice requiring the IDs. Such IDs will be destroyed as soon as the need for the ID has expired. Depending on the program, some IDs may need to be retained for a period of time for legal and financial purposes beyond the immediate purpose of the policy and practice. For example, IDs may need to be retained after the life of a grant to prove expenditure responsibility to government officials in the case of an audit. Check with Legal and Finance for any legal or finance record retention requirements.

V.1.1 (2013-03-14)

Illustrations

The following discussion is closed.

There are obviously a lot of things to talk about and if you aren't interested in this piece of it please feel free to start a new section with your discussion point/question/concern/etc. As you can probably see both here and on some of the other policies and draft pages we rolled out we're trying the idea of having illustrations and light humor in the text. These are not in anyway 'set' and may not appear in the final version if they're not appreciated. Legal documents tend to be lengthy, weighty and difficult to read (and rarely read at that) especially when you consider how many sites the average user visits. We want to make these documents as accessible as possible to as many people as possible. We hope to keep everyone's attention with the illustrations and a bit of levity. This is especially the case in the privacy policy but we've seeded them in a couple other locations as well. Do you like them? Hate them? Any specific ones work well or not work well? Should we think about another scene for a specific area? Jalexander (talk) 23:07, 3 September 2013 (UTC)

> I think the icons in the Privacy Policy are fantastic. Clear, and highly useful for navigating sections. The illustrations in both are fun, and I generally like them, but they're less useful for communicating the subject of the section. The top of the document says Rory is there to help explain the policy, but it doesn't feel like he's a narrator, more like an adornment. I think he should either be more tightly-integrated (perhaps with full SVG and color) or done away with in the name of simplicity. Steven Walling (WMF) • talk 05:18, 4 September 2013 (UTC)
>
> > I know color etc is an option for the final, it was just sketches now as the intro. Are you thinking more 'narration' ? Jalexander (talk) 05:20, 4 September 2013 (UTC)
> >
> > > Yeah I think if there's going to be a character, narration is probably more useful. Having to describe each section by putting it in a caption for the character to say is probably a good exercise in distilling the policies. Steven Walling (WMF) • talk 05:31, 4 September 2013 (UTC)
> >
> > The sketches of Rory are actually also meant to be up for community feedback -- the sketches are meant to be a start (that's actually why he is not in color and is unfinished). Final drafts of Rory will only be completed once community input has been obtained. We'd love to hear how he could be better utilized. Do you (the community at large) like the proposed sketches? Do you have ideas as to what else he should be doing to illustrate the concepts in the policy? What kind of narrative can we give him to bring the policy to life? How he could be better integrated? Privacy policies are notorious for being unreadable and hard to relate to. We hope that, with the community's assistance, Rory will be able to help with that. Mpaulson (WMF) (talk) 07:07, 4 September 2013 (UTC)

- **Note:** Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 20:44, 3 December 2013 (UTC)

Who's we?

The following discussion is closed.

"We will be accepting community comment until 15 January 2014. We look forward to comments on any aspect of the draft." ← Who's we? --MZMcBride (talk) 04:56, 4 September 2013 (UTC)

> Hi MZMcBride! "We" refers to the Wikimedia Foundation. This draft was the result of a collaborative effort between different departments, and coordinated by LCA. But the draft is not and cannot be complete without community input. We hope to hear from you during the community consultation period between now until 15 January 2014. During and following the community consultation period, we will be editing the draft presented today to reflect community suggestions and concerns, as appropriate, and then present the final draft to the Board for discussion and approval. Mpaulson (WMF) (talk) 05:15, 4 September 2013 (UTC)

A general aside: thank you so much for organizing these thorough public discussions and taking all of the feedback into consideration. I am learning a lot from this; and other community processes could as well. Including most of our global RfCs. –SJ talk 21:55, 24 October 2013 (UTC)

> Thanks Sj! The documents we introduce to the community are only a starting point. We learn so much from the community's participation and feedback during this process, and any resulting policies are better for it. =) Mpaulson (WMF) (talk) 22:15, 24 October 2013 (UTC)

- **Note:** Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 20:45, 3 December 2013 (UTC)

Wikipedia Day 2014

The following discussion is closed.

"We will be accepting community comment until 15 January 2014." ← What happens after January 15? Is there a public timeline anywhere? I assume at some point the Board has to approve the policy. --MZMcBride (talk) 04:57, 4 September 2013 (UTC)

> Hi MZMcBride! This draft is just that, a draft. We are working towards completing a final draft that has gone through vigorous interdepartmental and community feedback and will present that eventual draft to the Board for their review and discussion. The draft presented today will be reviewed and revised throughout the community consultation period in light of community feedback. After 15 January 2014, the draft will undergo any final revisions based on community feedback that

are still needed and then will be presented to the Board for discussion and potential adoption. Hope that helps! Mpaulson (WMF) (talk) 05:31, 4 September 2013 (UTC)

- **Note:** Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 20:45, 3 December 2013 (UTC)

Protect your access

The following discussion is closed.

Should contain something alla: 'users with these responsibilities will do the utmost to protect their accounts against unauthorized access, report immediately when they are aware such access has been compromised and follow the current agreed upon standards of usage of the account', the latter indicating that a user should use https if so defined in the current rules for checkuser access for instance. So i want to express that users can be assured that these people have a certain set of rules that they need to follow in order to be checkuser for instance, other than the 3 requirements of 18, ID'ed and pledged to confidentiality. TheDJ (talk) 07:01, 4 September 2013 (UTC)

Hi TheDJ! Thank you for your suggestion. Some of your concerns are actually addressed in the Confidentiality agreement for nonpublic information already.

As to your first suggestion, users with these responsibilities must "Comply with the Privacy Policy; the Access to Nonpublic Information Policy; and any other applicable and nonconflicting community policy relating to nonpublic information" and "Refrain from disclosing nonpublic information to anybody, except as permitted under those policies". Do you think adding another requirement that they must generally strive to protect their accounts against unauthorized access in addition to the requirements I mentioned above would be beneficial?

As to your second suggestion, they also have the duty to report disclosures under the terms of the confidentiality agreement -- they must "Notify check-disclosure at wikimedia.org and provide an explanation within 10 days if [they] disclose nonpublic information to outside parties, such as law enforcement" and "in case of a violation of this agreement, including improper access, use, or disclosure of nonpublic information...[they] will notify the Wikimedia Foundation about the violation immediately".

And finally, regarding your third suggestion, there are currently discussions within the Foundation as to how we can provide more secure connections to users with access to nonpublic information, but a perfect solution has not yet been found. https is certainly an option, but not one that we can apply everywhere. For example, https can actually hinder a user's ability to access in certain countries, like China. Your suggestion is a good one and one that we would like to implement in the future once we have methods of providing more secure access to users with these responsibilities (and hopefully all users eventually). Mpaulson (WMF) (talk) 18:13, 11 September 2013 (UTC)

In hindsight, I don't care as much about those 3 specific things, they could be internally documented. I want to make it clear to readers that the people who have this access to private material are required to act following the operational guidelines that are set for their specific 'position'. If you have "Minimum requirements for community members applying for access to nonpublic information rights", then (a) is a eligibility requirement for the functionary, (b) is an identification requirement on the functionary, (c) is an ethical agreement that the functionary signs with the foundation (which represents the community), (d) is a requirement onto the foundation about the proof talked about in a, b and c. My statement would have to express the 'burden' that is placed onto the functionary when he operates in his function to operate with the methodology that is expected of the function/office. (this could then include requirements on using https all the time for instance, protecting your password in general etc, but also for instance keeping non-public logs of actions for instance). We have trusted these users with some access and we require them to be careful with that access. When the library lends you a book, you don't bring it back all torn up. I don't know, it's complicated :D TheDJ (talk) 13:19, 23 September 2013 (UTC)

That's a fair point. What about if we change the last bullet point under (c) to "when and to whom they may disclose the nonpublic information and how they must otherwise refrain from disclosing nonpublic information to anybody, except as permitted under applicable policies" and add an additional bullets point saying "how they must safeguard their accounts from unauthorized access" and "when they must report disclosure of nonpublic information to third parties or improper access, use, or disclosure of nonpublic information"? We could would also add an additional bullet point in the confidentiality agreement under the "Protection of nonpublic information" section stating "Reasonably safeguard your account from unauthorized use." Let me know what you think of the additional language. Mpaulson (WMF) (talk) 23:47, 15 October 2013 (UTC)

- **Note:** Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 20:51, 3 December 2013 (UTC)

Why should copies of the photos ID be retained ?

The following discussion is closed.

While I can understand that the WMF would in some cases need to have confirmation of the identify of a volunteer, it is not clear to me why it should keep a copy of the actual photo ID. Whenever I need to be authenticated, I show my ID, someone checks that the information they have recorded is correct, then ticks a box on a paper form saying "ID checked" and confirms by signing it -- without keeping a copy of the ID. Usually, only banks require an actual copy of the ID. Why wouldn't it work ? In Switzerland, sending a copy of a photo ID is enough to authentify oneself in order to get access to most documents (medical record, bank accounts, criminal record). However, simply knowing the information printed on the ID does not open any such door. Could we setup the system in this way ? I know that the probability of someone misusing the data stored at WMF is small, but the potential consequences in case of problems are **huge**.

Another scheme that was suggested a while ago is that chapters (in countries where they exist), or a lawyer mandated by the chapters, should/could be used as a trusted 3rd party that would authentify such photo ID and send the relevant information to the WMF. This would have the added advantage that, for quite a few volunteers, they would not have to send any document to a foreign country (they may not even have to make a copy of the photo ID). Additionally, local people know what official photo IDs look like, and they could see the original document, reducing drastically any possibility of fraud. To me, this sounds like an appealing scheme, no ?

Finally, I am wondering about the following sentence:

> *The Wikimedia Foundation will not share submitted materials with third parties, unless such disclosure is (A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department*

I read that as "the WMF will not share submitted materials with third parties, except when it has itself approved to do so". That seems like a very weak protection. Shouldn't there be a explicit limitations of the cases in which such a transfer of material can happen ?

Thanks in advance ! Schutz (talk) 09:24, 4 September 2013 (UTC)

> FWIW, that's *not* an appealing scheme to WMIT, as clearly stated by our president and board. Of course if the WMF hired EU firms to handle such stuff many would be happier. --Nemo 21:04, 4 September 2013 (UTC)
>
> > Which problems do you see with this scheme ? Legal, practical, others ? Schutz (talk) 09:14, 5 September 2013 (UTC)
> >
> > > WMIT doesn't want and can't be an *agent* of WMF for anything. --Nemo 12:30, 5 September 2013 (UTC)
>
> Hi Schutz! One of the main reasons we are requiring identification from community members with this level of access is accountability. The information that is entrusted to these community members is very sensitive and knowing who has access to that information is a big part of working towards accountability. In the examples you stated where identification is required to get access to other information, you presumably get checked every time you try to access that secured information. Here, in situations covered by this policy draft, where the access is continuous, retaining a copy of the id submitted seems more logical that attempting to check someone's id every time they attempt to exercise their access rights.
>
> As to your second comment about whether it should be WMF that holds the ID, Nemo is correct in that chapters should not be seen as agents of WMF. That also doesn't help the community members who do not have chapters in their countries (or if in their countries of residence, chapters that are geographically close to where they reside). Appointing third-party attorneys or bodies to collect and hold the ids locally is administratively and legally challenging as well. Do we appoint an attorney in every location where there is a community member who submits an id? If the attorney is appointed, who is the attorney's client -- the community member or WMF? How would be ensure that all of these attorneys retain a copy of the ID properly (both in length of time and with proper security measures in place)? What happens if an attorney leaves practice and doesn't tell us or the community member? We believe that whatever risk associated with WMF's storage of the ids is considerable less than if the ids were stored by third parties.
>
> And finally, as to your third comment, I think some clarification about what kind of situations the sharing of these materials section is meant to cover will help guide this discussion. First, though, I'd like to note that there are limitations on when we can share the materials with third parties, specifically: "(B) required by law; (C) needed to protect against immediate threat to life or limb; or (D) needed to protect the rights, property, or safety of the Wikimedia Foundation, its employees, or contractors." Do you believe these situations are reasonable?
>
> I do understand your concern with regard to "(A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department" though. The reason why we included this was to address situations where a person helping with security of the materials is a contract employee who has signed a non-disclosure agreement with the Foundation or if we hire a company (who has signed a non-disclosure agreement) to help secure materials submitted electronically and they have to handle the materials in the course of helping us. The point of the Foundation's non-disclosure agreements with these sorts of parties would be to secure similar or greater protections than those promised in this policy. Does that make sense? If so, do you think the language of (A) could be changed to make this clearer?
>
> Hope this helps and look forward to hearing more of your thoughts on these topics. Mpaulson (WMF) (talk) 20:13, 11 September 2013 (UTC)
>
> > Sections (A) and (D) jumped out at me as well. They both appear to offer quite fragile protection for those submitting "non-public information" to the WMF - which is, you might agree, ironic. I think A should be tightened up to narrow the circumstances in which information is shared (such as including provisos that it will not be for commercial use, and that no outside entities will retain a permanent copy of any personally identifying information). I think D also has holes

big enough to drive a truck through, because "rights and property" of the WMF, its employees and contractors is a pretty broad category. Does that mean if permanently deleting the data from the hard drive of a contractor might damage that contractors property, the policy allows them to retain the information? I understand that the natural inclination of attorneys representing a client is to draft as broadly as possible in favor of the client, but that is the wrong impulse when considering the responsibility of the WMF to protect the identifying information of both readers *and* volunteers. Since the volunteers are potentially sharing much more sensitive information, a little more weight on protecting them needs to be added to this policy. Nathan T 19:25, 14 October 2013 (UTC)

> Hi Nathan! Thank you for sharing your thoughts. As to (A), what do you think about tightening the language to something like this: (A) permitted by a non-disclosure agreement that (1) has been approved by the Wikimedia Foundation's legal department; (2) allows for only non-commercial use of the submitted materials; (3) allows for use by the recipient of the submitted materials in accordance with the Wikimedia Foundation's instructions; and (4) obligates the recipient of the submitted materials to return or destroy all copies of the submitted materials in its possession within a reasonable time following the recipient's need for the information.
>
> And as to (D), I understand why you think the provision is broad. It is meant to be, but not because we are trying to draft broadly in favor of WMF as our client. We wrote it broadly because it was meant to cover unlikely and, to a certain extent, impossible-to-predict scenarios that can be hard to enumerate. I admit, I'm a little confused by your example of how this provision could be used. If permanently deleting the data from the hard drive of a contractor would damage that contractor's property, that doesn't mean that the policy allows them to retain the information. Clause (A) would cover how we were permitted to give access to the information to the contractor, but not how long they could retain the information. Clause (D) covers completely different scenarios where we would be permitted to share information. For example, in the unlikely scenario where our building was broken into and our equipment was stolen or where our computer systems had been compromised and we had a good reason to believe that it was someone whose personal information we had, we would be permitted under this clause to report that person to the appropriate authorities. Again, it's hard to imagine every possible scenario where this clause may be helpful. I frankly hope we never, ever have to use the clause. We do not take the disclosure of personal information lightly. In fact, we are loathed to disclose information short of being legally compelled to do so or for safety reasons. That said, we're very much open to editing (D) in a way that would better illustrate what that clause is trying to cover and I'd love to hear any suggestions you may have. What about something like this: (D) needed to protect the safety of others or WMF staff, contractors, systems or property?
>
> I look forward to hearing your thoughts on my suggested revisions as well as any suggested revisions you may have. Mpaulson (WMF) (talk) 19:54, 16 October 2013 (UTC)
>
> > You still have not answered the question of why the ID has to be retained over retaining the Data in it. And I for one will never, ever accept the property clause of this proposal. That is simply unacceptable. Snowolf How can I help? 20:07, 17 October 2013 (UTC)
> >
> > > I second Snowolf's sentiment; I don't think our data should be used for non-commercial purposes, either. I also suggest to obligate any recipient of our sensitive personal information to return or destroy all copies *immediately* following their need for it. On a related note, why would you share this sort of personal information with anyone at all? I don't really see any need for any contractor or WMF staff member except perhaps two or three people (take Philippe and Geoff from Snowolf's example above) to have access to it. odder (talk) 21:08, 17 October 2013 (UTC)
> > >
> > > > Outside counsel is the only thing I can think of. Snowolf How can I help? 21:28, 17 October 2013 (UTC)
> >
> > "You still have not answered the question of why the ID has to be retained over retaining the Data in it." I think we'd probably be OK with simply retaining the data. We'll have to think about it some more, but the ID portion of the proposal was mostly based on past practice. Would keeping data, rather than the ID, resolve your other concerns about us collecting this data? -LVilla (WMF) (talk) 22:43, 25 October 2013 (UTC)
>
> On the question of "property" as a "loophole": the idea here is really primarily about our technical infrastructure; e.g., if a volunteer developer who we have ID'd starts attacking the site, we'd like to be able to use this information to help identify them and protect the site. So does it feel more narrowly tailored if we replace "property" with "infrastructure"? -LVilla (WMF) (talk) 19:57, 1 November 2013 (UTC)

- **Note:** Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 20:51, 3 December 2013 (UTC)

CheckUser policy

The following discussion is closed.

As already addressed here, let me reiterate my remark (that still remains) about the revelation of **the link** between an IP and an account, as it is a

compound of private and public data.

Aside from this point, I am happy with the changes and the new layout of the page. Elfix 08:00, 5 September 2013 (UTC)

> Hi Elfix! Just to be clear, are you referring to the the link between logged-in accounts and anonymous accounts in situations like sock-puppet investigations? If so, I think the Privacy Policy draft most directly addresses this situation in the To Protect You, Ourselves, and Others section...specifically: "We may need to share your personal information if we reasonably believe it is necessary to enforce or investigate potential violations of our Terms of Use, this Privacy Policy, or any Foundation or user community-based policies." To a certain extent, public inference of the links between particular IPs and accounts are unavoidable in sock-puppet investigations and are permissible due to the sentence above. I do understand your concern that it is not as clearly stated with in the Access to nonpublic information policy draft or the Confidentiality agreement for nonpublic information as to whether the community members handling these investigations are permitted to disclose this information in the course of their investigation. I'd love to have this stated more clearly. Do you have any suggestions as to how we could make it clearer in either the Access to Nonpublic Information Policy draft or the Confidentiality Agreement draft? Mpaulson (WMF) (talk) 19:28, 11 September 2013 (UTC)
>
> > Thank you for your response. I didn't pay enough attention to the bit you are quoting, and it is, I think, clear enough. Thanks! Elfix 21:33, 12 September 2013 (UTC) However, in "We may need to share your personal information", the use of the "share" verb may not be clear here (share with whom?). Elfix 18:50, 13 September 2013 (UTC)
> >
> > > Yes, the language in the Privacy Policy draft is relatively broad because it's trying to cover any possible person/entity that may have to be alerted depending on the type and severity of the alleged violation committed by literally anyone who can access the Wikimedia Sites. I'm not sure if there's a way for us to do an exhaustive list to cover every possible scenario. We do try to be more specific in the Access policy draft about to whom and under what situations community members with access rights may disclose information to though. Mpaulson (WMF) (talk) 00:36, 16 October 2013 (UTC)

I have a follow-up hypothetical question for you. The case of the UK where random IPs in dynamic ranges typically don't do anything other than reveal you're in the UK is quite clear cut. However, let's say that a person's IP reveals private information about them (e.g. they're on 130.88.0.0/16, a range owned by the University of Manchester). In terms of the policy, does this change the above advice that it's permitted to disclose that IP to someone in the case that they, say, want to write an abuse complaint to the University of Manchester? --Deskana (talk) 09:25, 15 October 2013 (UTC)

> Hi Deskana! Thank you for your question. Do you mean whether it would be ok for a community member with access rights to disclose a nonpublic IP that is specific enough to identify that the IP falls within a range owned by the University of Manchester and is associated with a user account? It would be ok if the disclosure was made as part of an investigation of potential violations of a policy and the IP was disclosed in the an abuse complaint "to assist in the targeting of IP blocks or the formulation of a complaint to relevant Internet Service Providers" (that latter if UM was also the ISP). Otherwise, no, they should not disclose the IP. Did I understand your hypo correctly? Mpaulson (WMF) (talk) 00:36, 16 October 2013 (UTC)
>
> > Perhaps a more specific and common situation: IP address provides some sort of information about the user (e.g., it's a business IP, and researching it through WHOIS will identify the business). There are a pile of socks, and there are no good users on the IP. Standard practice is to at least softblock the IP while also blocking the socks. However, it takes no imagination at all to make the association with the IP address and the socks just by looking at the CU's block log. So....is the CU violating policy by blocking both the socks and the IP? Risker (talk) 02:27, 16 October 2013 (UTC)
> >
> > > Hello @Risker:, this is a tough situation. For the same reason that Michelle explained above, it's allowed under the current version of the policy. However, upon a closer reading of the new draft privacy policy and access to nonpublic information policy, this is not addressed directly. To make it clearer, we could add to "Use and disclosure of nonpublic information", section (b):
> > >
> > > > *Disclosures of nonpublic information may be made to: ... the public, when it is a necessary and incidental consequence of blocking a sockpuppet or other abusive account; ...*
> > >
> > > This would make it acceptable under the privacy policy/access policy for CheckUsers to conduct the type of blocks that you suggest. Of course, projects could also set a higher bar in their local CheckUser Policy, if they don't think this is appropriate. This is a tough question, but the policy can be accommodating if its necessary for CheckUsers to do their job. Thanks, Stephen LaPorte (WMF) (talk) 21:13, 1 November 2013 (UTC)

- **Note:** Given how long this thread has been stale and the fact that it appears to be resolved I'm going to archive this in a couple days unless reopened. Jalexander--WMF 20:54, 3 December 2013 (UTC)

Data retention forced by what law?

The following discussion is closed.

Current draft says the collected ID will be retained for 3 years. I'd like to ask this measurement is forced by what law. In my country the data retention criteria are fixed in written law, and unless the data retention is required by law the data must be destroyed immediately the purpose of data collection is satisfied. Data retention without legal basis will be only the risk that the data would be compromised. There are several accidents that personal information of 35+ millions of people are leaked. If the data retention is based on US law, please let us know where the legal basis is, and if not, please don't retain the data. Best regards. – Kwj2772 (msg) 14:34, 25 September 2013 (UTC)

> The same here in Italy, data must be destroyed *as soon as possible* on request. --Vituzzu (talk) 18:30, 14 October 2013 (UTC)
>
> I doubt the specific time period is mandated by law, although there are various statutes of limitation - many of which in California are three years or less. I'm just speculating, but other circumstances that might dictate data retention times are contracts, grant terms, government funding, participation in certain state or federal programs, etc. Unlike European and other jurisdictions, the U.S. does not have a general limit or prohibition on retaining private data. And while many users live in jurisdictions where those rules apply, they do not govern the behavior of the WMF. Nathan T 19:37, 14 October 2013 (UTC)
>
> > But still I'm subjected to EU law. --Vituzzu (talk) 10:46, 15 October 2013 (UTC)
> >
> > > Hi Kwj2772, Vituzzu, and Nathan. Thank you for your questions. While there are data retention periods that are mandated under US law for specific situations (such as tax purposes, retention of client files, etc.), Nathan is correct in that there is no general law in the US that governs data retention periods and WMF is not subject to EU retention laws. Organizations are free (absent specific situations where particular laws apply) to set their own data retention periods for different types of data. Mpaulson (WMF) (talk) 17:49, 18 October 2013 (UTC)
> > >
> > > > Even if you're not subject to EU laws on data retention, it might be well worth looking into them and perhaps adopting some of the regulations; there are many stewards, checkusers, oversighters and OTRS members who are EU citizens, and I'm sure some of them would like you to adopt these higher standards even if you're not obliged to do so by U.S. law. odder (talk) 17:59, 18 October 2013 (UTC)
> > > >
> > > > > I would be interested in hearing from you guys about what you think would be an appropriate retention period? If you have thoughts on this issue, please leave them in the retention thread. (I'm trying to keep the responses on that topic in one place so they are easier to track.) Thanks! Mpaulson (WMF) (talk) 22:56, 25 October 2013 (UTC)

- **Note:** Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:02, 3 December 2013 (UTC)

Re-identification and retention of data vs. the NSA

The following discussion is closed.

I have identified to the Foundation a couple of years ago upon receiving access to OTRS, and my identification has been confirmed by a WMF staff member. Therefore, I cannot see anything that changed in those past few years that would require me to re-identify with the WMF, and send them a scan of my ID again.

I am also very concerned and feel deeply uneasy about (re-)sending a copy of my ID--which is probably one of the most delicate information the WMF can hold--to an organisation in a country where countless government agencies can force them to reveal any and all information they want, or even get the information without a court's approval or the subject's awareness. (Yes, I'm looking at the U.S., the recent scandals around the NSA, and the worryingly broad scope of the CIA and other intelligence-gathering organisations.)

If a re-identification or change of the current policy is required, I would prefer to be able to identify to an organisation, group or an individual acting in professional capacity in a jurisdiction which guarantees the best possible protection of my personal information (see data retention policy issue brought above by Kwj2772), and where I will have the ability to protect my personal liberty in the most effective way possible, without having to spend tens of thousands of dollars and fight against the ever-expanding appetite of government intelligence agencies. odder (talk) 16:12, 14 October 2013 (UTC)

> This policy will make most of most active users leave the Project, I wonder who will eventually checkuser, oversight, etc upon these basis.
>
> - These changes are made by a completely USA-centric perspective, without any care for other Countries' jurisdictions (for instance the three-years terms violates Italian law) but also different cultures (for instance in European countries law tends to avoid lawsuits and *subpoena is completely insane by our perspective*). You shouldn't forget users living outside USA are subjected to their respective countries' laws.
> - These changes make the policy even more blurry, on a theoretically basis everything can be meant to *prevent damages to WMF's properties*.
> - Also, a confidentiality pledge is not bad but still it doesn't take into any consideration the whole World outside USA, both the agreement and the way to sign it might have no value at all for people living outside USA.
> - This new version gives legal value to "normal" emails, I don't know if this might have any value in USA, but this is utterly ridiculous here in EU.
>
> Finally I have a simple question: each change is supposed to fix some practical problem, so, **which problems are supposed to be fixed by these changes?**
> --Vituzzu (talk) 17:35, 14 October 2013 (UTC)

> Hello @Vituzzu: Michelle has provided more detail on why these changes are being considered below, at Rethinking the access policy: Response to recent feedback. Does this answer your question? Stephen LaPorte (WMF) (talk) 21:39, 1 November 2013 (UTC)

- Anything could be argued to be a damage to WMF's properties. If I go out and criticize the WMF, I am damaging its properties in a way. I do not think that I would be able to continue serving in my capacities should such a flimsy policy be implemented. I was already uneasy about submitting identification when I did so some years back, and that was with the assurance that it would be destroyed after my identity was confirmed. My concerns are magnified by the idea of the documents being retained. I recall a lengthy thread on some OTRS mailing list in 2008 or 2009 about the processing of identification informations, where several volunteers were raising questions about the then current practices. Some of the points made then should be taken into account now, if the WMF wishes to go ahead with this. **Snowolf** How can I help? 18:08, 14 October 2013 (UTC)

> It's also funny to read *WMF employees and contractors...hey I'm a contractor making a research about the way different countries print IDs!* Seriously, nobody knows how the fuck is hard to sue one of these unfaithful contractors from the other side of Atlantic or Pacific Oceans? Also, though my main question still is "why is this change needed?" I have also another question: "why so few announcements have been made in comparison with the asphyxiating spam we are used to receive for every futile change in some useless MW's functionality?".
> --Vituzzu (talk) 18:28, 14 October 2013 (UTC)

> I'm more concerned about id theft and data leak than anything else. I don't like the idea of somebody storing a scan of my driver's license, which could easily be used for nefarious purposes by malicious individuals, on a networked server. Would the data be taken from the "secured" inbox, encrypted, and then placed into an air-gapped server? Reaper Eternal (talk) 18:40, 14 October 2013 (UTC)

> > That is my worry too. I also don't want the printed stuff to be in a some office locker. It should be in a serious safe. We should have a list of those with access, etc.. The issue of the air-gapped server was discussed at length in the otrs mailing list in a thread from I belive 2008 or 2009. I wish I could find it as the point made there are just as relevant now. **Snowolf** How can I help? 19:31, 14 October 2013 (UTC)

> > > The discussion you seem to have in mind took place in February 2011. You can see the relevant thread on Wikimedia-l (then Foundation-l) here (http://lists.wikimedia.org/pipermail/wikimedia-l/2011-February/110390.html); there was also a discussion on the OTRS wiki cafe (https://otrs-wiki.wikimedia.org/wiki/Caf%C3%A9/Archive_6#Identification_of_OTRS_agents). This post on Foundation-l (http://lists.wikimedia.org/pipermail/wikimedia-l/2011-February/110392.html) mentions threads on the private otrs-en-l and otrs-permissions-l mailing lists, but I am no longer subscribed to any of them, so I can't check the archives. I hope this will help with your search. odder (talk) 20:19, 14 October 2013 (UTC)

I can only agree with odder, Vituzzu, Snowolf and Reaper Eternal. This proposal is highly outrageous. Like Vito I can't see any problem which would be fixed by this. I plan to resign as a steward if it passes. Some complaints, in addition to those already mentioned above:

- At first it is stated (in "(d)(i)") that the data will not be shared by the WMF etc. bla bla except if *(A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department; (B) required by law; (C) needed to protect against immediate threat to life or limb; or (D) needed to protect the rights, property, or safety of the Wikimedia Foundation, its employees, or contractors*. As wide-ranging as that is formulated, it st)ll gives some "severe" criteria. Then in the next section ("(ii)") however we read *"the Wikimedia Foundation or a user community committee will need to contact a community member who formerly had access rights about his or her usage of those rights. For example, the Arbitration Committee may need to complete an ongoing case they are examining or the Wikimedia Foundation may need to notify you of receipt of a legal document involving that community member."*
  - That the Foundation may need to contact a user about how/why he used CU in a certain way or so certainly does not always mean that they may need to do it to protect the Foundation's glorious property. Nevertheless just before such a requirement was established. So why is such a fishy reason used for justifying keeping the data? Even more dubios the next reason:
  - What the heck is a "user community committee"? The next sentence of course suggests it is "the Arbitration Committee". What the heck is "the Arbitration Committee"? There is no global arbcom or anything. Just some projects happen to have one. This proposal was clearly written by someone focussed on enwiki.... but apart from that, it sounds like any community may just establish a committee that then uuurgently has to ask some questions. How nonsensical. If at all, there need to be clear criteria for such an (arb?)com - which criteria it must fulfill (e.g. selection method, identification of members themselves?) in order to be considered to be allowed access to such data.
  - Additionally, how would such a "the Arbitration Committee" contact the user? (It also of course seems like we must assume someone who is not active anymore, as otherwise he could simply be asked on his talk page or by mail. Right to vanish?). Get the address and mail him? Will WMF visit or sue him on behalf of "the Arbitration Committee" until he answers?
  - "The Foundation may need to notify you of receipt of a legal document involving that community member". This sentence totally makes no sense. You == "that community member"? And what a legal document? A legal document calling for "that community member" to be arrested?
- The "destruction process" is also total bogus. A user who no longer has CU/OS access should notify stewards, who then inform the Foundation. First, stewards notice anyway when CU/OS removal happens, because they do it. Second, it reads like the data will only be destroyed if the user "notifies stewards" at all. Can a steward just tell the Foundation sua sponte that someone lost CU/OS or only when the user himself requested it? Third, why stewards at all? They are volunteers, they might also simply forget to impart the "wish for destruction" in a case, etc. If this outrageous proposal succeeds at all, there **needs** to be a qualified WMF staffer who watches Special:Log/rights for removal of CU/OS/steward and is also contactable by users who lose this access, just to be sure, and who sees to it then that the data is really destroyed after the prescribed time. And then not only "in a timely manner following the three (3) year period" but immediately! It is barefaced to say data is stored for maximum 3 years after the loss of access, and then only execute this "in a timely manner" i.e. when we want.

--MF-W 21:57, 14 October 2013 (UTC)

> I fully agree with the opinions expressed above me in this section, but I'd like to expand on the problem with giving power to a "user community committee" in this case. There are very, very few projects which have an ArbCom or similar body (and no such body exists at the global level), so these groups shouldn't be included in any policy as the norm. If they are ever mentioned, it should be as an after-note in a different sect)on explaining special cases.

> On this note, the role of a "user community committee" isn't defined at all here. Will they actually have access to scans of ID? It seems to imply that the Foundation is keeping them around so they can look at them later... to contact me or "complete an ongoing case". What does that mean? Can I go to lessthantencontributors.wikipedia.org, become an admin and arbitrator, and then get access to all identified people's documents? Why would an arbitration community, or a "user community committee" even need that sort of information when filling the definition of their role? Google defines arbitration as "The use of an arbitrator to settle a dispute", not "A body who looks at confidentially-submitted IDs and stalks former contributors". Some clarification here would be useful. Ajraddatz (Talk) 23:31, 14 October 2013 (UTC)

- As can be deduced from my contributions, I am a resident of the state of California, so there is no getting around California state law in my case. I can see where this proposal comes from, and I believe there are valid points here. But I believe in some areas that this proposal goes too far. There are several loopholes as mentioned by the others above. I still have yet to go through this in fine detail, but one thing that doesn't strike me too well is the clause saying, in effect, "if you leak private data, we will sue you." Of course, I believe that in some cases legal action may be appropriate, such as a steward/CU willfully violating people's privacy. But the way it's written, it implies that not even our most trusted functionaries are ... trusted, and that honest mistakes will be swiftly and soundly punished by consequences in real life. If that is to be the case, then we might as well have WMF take over all functionary positions, because I don't think there will be many takers for such a *volunteer* role. Functionaries are editors, and their privacy should be protected too. --**Rschen7754** 23:26, 14 October 2013 (UTC)
- I'm also fairly alarmed by this change, on two fronts. **First**, the general idea of the WMF keeping copies of documents of mine that could be used to do everything from open a bank account to getting a duplicate passport is alarming. In the cases of other organizations that have such documents from me, the organizations have track records and demonstrable processes for protecting the data, both physically and electronically (as well as there usually being established legal/governmental processes that hold the organizations to their promised non-disclosure and protection). The WMF, on the other hand, proposes to get these documents from us with a promise of, "We'll totally lock that filing cabinet and password-protect the file!" Unfortunately, organization at the WMF often seems to be lacking, and I simply find myself unable to muster enough confidence in its ability to make this one particular procedure bulletproof, this one time, the first time.

  Second, the idea that they won't disclose my personal information, except when they decide they can disclose it to whoever they want ("permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department") or when they decide it's in their best interest ("needed to protect the rights, property, or safety of the Wikimedia Foundation, its employees, or contractors"), amounts to "so, we won't give people your passport, except when we will, which might be pretty often, who knows?"

  I was and am perfectly fine with letting someone at the WMF check over my documents to verify my identity (as, indeed, they have already done). But before I'm comfortable with them keeping copies of it for their own purposes, I need to see far, far more detail about a) how my rights (not the WMF's) will be protected as far as who gets copies of my information, and b) how, exactly, my data will be protected. "We'll put a padlock on the cabinet" isn't adequate; I'm looking for something more like "We have designed storage procedure X and had it audited by independent security firm Y, which verifies that this procedure is state-of-the-art and resistant to both tampering and hacking to a level standard in the data-protection industry." The contents of people's passports, identity cards, or driver's licenses isn't the sort of thing you can protect using "agile" development where you start with something that sort of works and then iterate to improve when you find bugs. You need to have proven security from the very first moment, because if this goes wrong, it won't be annoying for the people whose identities are stolen, it will be *catastrophic*. Fluffernutter (talk) 00:29, 15 October 2013 (UTC)

- Man9`good points. On the other hand, WMF has to have some way of knowing who tools holders are (especially CU), and it should be a bit more than WMF staff memory. Perhaps a one-time ID check and registering a name somewhere (plus perhaps other data, such as date of birth, but not full ID scans) would address the concerns above? Pundit (talk) 05:15, 15 October 2013 (UTC)
- I **strongly oppose** this. I echo Snowolf's concerns and with the security breach at Labs, I do not feel comfortable with this change. Echoing what Vituzzu said, I would be one of these users who would leave. Elockid (talk) 22:33, 15 October 2013 (UTC)
- I am in agreement with my colleagues above. Furthermore, I understand why certain contracts mention the possibility of legal action, but these contracts then must include compensation for the signing party. Just like I refuse to sign publication waivers that make me solely responsible before the law if some madman decides to claim my images as his and sue, I feel uncomfortable with the present framework. People who have to answer before the law must know precisely when they are within their purview or not, they must enjoy legal support in case of problem, and they must be paid for the trouble. I am a volunteer here, and while I do pro bono work out of idealism, the pleasure I derive from the very act of contributing is also a factor; having second thoughs about prosecution in the USA for every action I take makes contribution less enjoyable, and there is a point where a contributor, without making a big fuss about it and without necessarily hitting a particular red line, will decide that the boat is overloaded and shrug off their commitment to the projects. Rama (talk) 06:35, 16 October 2013 (UTC)

Explain data retention in the policy itself

I think it would be very helpful for a complete and clear statement from the WMF, within the policy itself, on why identification is necessary and separately why it is necessary to retain hard copies of government-issued identification of volunteers. Many non-US countries have a very different culture when it comes to personal and private information, and are likely to have (and already are having, in some cases) a much stronger negative reaction to this than Americans might overall. It's unfortunate that the policy sort of glosses over the justification for data retention without making a really strong argument in favor of it, so perhaps Geoff and his team can remedy that? **Nathan** T 19:41, 14 October 2013 (UTC)

> Nathan, I know you've already seen this, but to anyone else following this thread, you may be interested in the discussion below regarding why we would like community members with access rights to identify. I'd also like to note that we are open to the possibility of retaining only identifying information about these community members rather than copies of identification documents themselves. We'd love to hear from other community members on this subject. Thanks in advance (and specific thanks to you, Nathan, for your patience as we respond to everyone's input.) Mpaulson (WMF) (talk) 23:18, 31 October 2013 (UTC)

Who needs to identify at all now?

>>Any community member who has been granted access rights and has not previously identified under the previous "Access to nonpublic data" policy (adopted 2007) has sixty (60) days to meet the Identification Requirements of Section 2(b) and the Confidentiality Requirements of Section 2(c) of this Policy."<< Do such users still exist? Afaik nowadays everyone who has access to CU/OS should be listed on IN. --MF-W 22:12, 14 October 2013 (UTC)

> If I remember correctly, there might still be some OTRS agents who have not identified to the Foundation, as this was never a requirement that was set in stone. There were some plans to force every OTRS agent to identify to the Foundation in February 2011, but they don't seem to have been put into action, in the end. odder (talk) 22:31, 14 October 2013 (UTC)

> > When I joined OTRS in September/October 2012 I did not have to identify, though I did a few months later for my OS flag. --**Rschen7754** 23:11, 14 October 2013 (UTC)

> > > Hi MF-W, odder, and Rschen7754. I know that you have seen this related discussion, but I wanted to point out to others who might be following this thread that the OTRS question is still being discussed and we'd love to hear more opinions about whether OTRS members should be included. As for other types of community members who may not have yet identified, this clause is meant to cover anyone who has access rights who may have not known (for whatever reason) that they had to identify under the 2007 policy. Mpaulson (WMF) (talk) 23:37, 31 October 2013 (UTC)

Enwiki ACC

I've notified the enwiki ACC members since this affects us too. Reaper Eternal (talk) 00:46, 15 October 2013 (UTC)

> Thank you Reaper, if you want me to send anything out to them please let me know, it was only my list since I was reminded about them but I won't beleaguer the point if not helpful. Jalexander--WMF 02:21, 19 October 2013 (UTC)

WMF?

It's been a few days and other questions have been answered, but not the more concerning questions above. Does the WMF plan to edit the proposal to address these concerns, or should we be making our decision on whether or not to reidentify based on what the proposal is, since the WMF does not plan to address the concerns above? --**Rschen7754** 01:59, 19 October 2013 (UTC)

> I would encourage you to wait before making any decisions like that. We want to come up with a good policy that as many as possible are happy with. Michelle has been answering questions from her sick bed at home this week (and I imagine you will see a bit more over the next couple days) but we plan to get together early next week in the office to discuss some of the unanswered questions. The consultation is scheduled to last at least 3 more months (there is no hard deadline, if we're not done then we keep going) exactly so we don't need to rush this. Given the experiences with other policy discussions (ToS/Privacy policy etc) I think we can expect that this is just the start of the discussion and edits (both small and major) to the document(s) in the weeks to come. I will be making sure that I stay on top of the legal team to both strongly think about, and answer, all of the concerns being brought up. Jalexander--WMF 02:20, 19 October 2013 (UTC)

> > Rschen's concerns are well justified. Over the last few days, Mpaulson has been addressing a lot of minor concerns that don't require pretty much a complete rewrite of the policy, and has even implemented one edit to the policy. At the same time, all of the major concerns have been completely ignored. It just feels like the WMF wants to implement it very close to its current form, and is consequently ignoring any complaints which would require a big change. Thanks for clarifying that these are being looked into and will be addressed... if that's what you're saying. Ajraddatz (Talk) 02:31, 19 October 2013 (UTC)

> > > That is indeed what I am saying :). I know that people are frustrated by a bunch of pieces and we are in no way trying to ignore any of it (I can't think of anything that isn't up for discussion) Jalexander--WMF 02:34, 19 October 2013 (UTC)

> > > > I've appreciated the way the largest questions have been thoughtfully addressed. Thanks to the legal team for the thorough and ongoing replies. --SJ talk 21:55, 24 October 2013 (UTC)

> > > > > Hi Rschen. I just wanted to follow and let you know that we're responding to a lot of the big issues this week. Many of these responses are clarifications and ask for further response from the community. Once we hear from more members of the community on key issues (such as whether we should still be requiring identification at all, submission of identifying information rather than copies of identification documents, what kind of identifying information would be sufficient, what kind of verification of this information would be needed, what would be an acceptable retention period for such information, etc.), we will start making proposed edits based on the feedback. Mpaulson (WMF) (talk) 23:28, 31 October 2013 (UTC)

- **Note:** Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:03, 3 December 2013 (UTC)

Identification

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:05, 3 December 2013 (UTC)***

Would the photo ID have to remain valid for the duration of the time the rights are held? --**Rschen7754** 19:48, 14 October 2013 (UTC)

> Good point. Surely the WMF also needs to be notified on address changes etc. to ensure that all required data is always up-to-date! --MF-W 22:07, 14 October 2013 (UTC)
>
> > Great point, Rschen7754 & MF-W! We will add "inform the Wikimedia Foundation of any change to their name, address, or email address within a reasonable time following such change" to the identification section of the policy draft. We will hold off on addressing the photo ID remaining valid throughout the duration that the rights are held until we hear more input about whether copies of photo identification should be held at all. Thanks! Mpaulson (WMF) (talk) 22:50, 31 October 2013 (UTC)
> >
> > > Lol. I said this as a joke of course, in order to mock the ridiculousness of the proposal. The change (https://meta.wikimedia.org/w/index.php?title=Access_to_nonpublic_information_policy&diff=6222708&oldid=6222528) of course only adds to the ridiculousness, so you could as well already "address the photo ID remaining valid" while there is finally the option to discuss sth useful like whether copies of photo identification should be held at all. --MF-W 11:59, 8 November 2013 (UTC)

Change of identity information

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:05, 3 December 2013 (UTC)***

What would be done in the event that the identity information of a person changes? I'd like a policy covering the following points:

- For those who currently hold access rights, documentation must be submitted; for those who previously held access rights (and whose information is still retained), documentation may be submitted.
- If a new ID document is submitted, WMF's copy of the old ID document will be discarded; if the submitted documentation of change is not an ID document on its own, both it and the old document will be retained until (if ever) a new ID document is submitted or the retention period expires.
- If a person who previously held access rights submits a new document, this does not reset the retention period.

I'll admit I'm not entirely sold on whether a copy of ID documents should be retained at all, but if it is, a policy on changing information is necessary. (As an aside, is there a reason the name of the policy is being changed from "access to nonpublic data" to "access to nonpublic information"?) MaxHarmony (talk) 21:03, 14 October 2013 (UTC)

> Hi MaxHarmony! These are all excellent points. I will make some proposed edits to the policy draft for your review. As for the name change, it was primarily for consistency. In the new privacy policy draft, the term "information" rather than "data" is used. Thank you for taking the time to make these suggestions. Mpaulson (WMF) (talk) 17:58, 18 October 2013 (UTC)

Valid for Supportteam-members with access to OTRS-queues?

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:06, 3 December 2013 (UTC)***

Does the section: *"Community members with access to any tool that permits them to view nonpublic information about other users"* include supportteam members with access to OTRS-queues?

If yes, what is the rationale of requesting to store a copy of the picture ID Documents and residence for Supportteam members. Best regards --Neozoon (talk) 23:16, 14 October 2013 (UTC) (identified member of the German Supportteam)

> Just a note that there is a discussion above here at OTRS_volunteers where Michelle commented and asked for some thoughts. This is something that is currently being discussed internally and having opinions here is very important in my opinion. In general we currently tell people as they join OTRS that they may have to identify (but have not been enforcing that), whether the policies should be merged or not is something I think should be discussed along with this policy as it should be addressed in it (even if it's an exception. Jalexander--WMF 00:25, 16 October 2013 (UTC)

Why a 3-year post removal retention period?

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active (including too the retention period) I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:06, 3 December 2013 (UTC)***

I can see retaining ID information for a period of time, perhaps 6 months to a year after removal (voluntary or involuntary), with a clause stating that information will be retained longer if there is an ongoing internal (WMF/Ombud) investigation; however, three years seems awfully long. I bear in mind the significant number of people with this level of access who are comparatively transient (e.g., students, those whose work requires travel or moving), so three-year-old data is probably fairly useless. Can we have an explanation of where the 3 year period came from? Risker (talk) 23:18, 14 October 2013 (UTC)

> Michelle? --MZMcBride (talk) 22:36, 20 October 2013 (UTC)

> > Hi Risker and MZ. Sorry about the delay. I had pneumonia and am playing a serious game of catch up this week. The reason why we had decided on 3 years is that when discussing potential periods for retention with the Ombudsman Commission, it seemed possible for an investigation concerning the actions of a community member with these kinds of access rights to still be ongoing 2 years after the community member in question had resigned their rights. This could be the case in a particularly complex investigation or one that did not come to the attention of WMF or the Ombudsman Commission until after the community member resigned their rights. That said, I understand that 3 years can be perceived as a long time and if the community believes that investigations of these kinds are all but rarely resolved in a shorter period of time than 3 years, I'm certainly open to hearing what they believe is a more reasonable length of time. Mpaulson (WMF) (talk) 21:34, 22 October 2013 (UTC)

> > > A maximum reasonable time I think would be 6 months after removal, and extended for an investigation as Risker suggests. At the same time, I don't see what benefit holding information for investigations would give anyway, and this gets at the complaint that this change is a solution looking for a problem. Are the functionaries so rogue and out of control and abusing of their rights that this has lead to multiple cases recently where having their personal information on-file would have solved the case, or at least allowed WMF to sue them? If the entire motivation for this change is so that WMF can sue all the crazy rogue functionaries, then all the rhetoric here about us being really trusted people whose input is desirable is just a farce. On the one hand, we're the cream of the crop (or so you'd think reading things like "community members who are in the valuable roles"), but on the other we're so naughty and prone to frivolous revealing of the confidential information we have access to that they need to keep our personal information so they can sue us. I think that before any more responses are given on specifics, the WMF legal team needs to finally answer the question of why this change is happening. Ajraddatz (Talk) 22:23, 22 October 2013 (UTC)

> > > > Hi Ajraddatz. Thank you for your input on what you believe to be a reasonable retention period. What do other community members think?
> > > > As to your other comments, please see the posting I have done on why we believe a change is needed and the possible solutions that we think we could pursue. We would love to hear your feedback on this issue. We recognize that this is a sensitive topic, but please believe that we are trying in good faith find solutions that work for the community -- and figuring out what's best involves a lot of discussion with the community, which is why we are having this discussion. Mpaulson (WMF) (talk) 22:11, 25 October 2013 (UTC)

> > > > > I think that's fair. I think someone suggested keeping the real name around for longer due to certain past cases, and I don't have a problem with that either. --**Rschen7754** 22:15, 25 October 2013 (UTC)

There are different answers for me depending on who is holding the records and for what clear purpose. For community investigations, zero, these are legal records I don't see why community bodies, which according to our long history have proven insecure, should hold them, when there can be no legally binding investigation by definition. For the WMF, zero, as again this is a system subject to unspecified future changes or a general loss of corporate memory (refer to many, many cases of private records of all sorts turning up in skips after company changes from wind-up through to office redecorating meaning someone lost track of the filing cabinets). If legal records of identity were held on an escrow contract of some sort, where a leak or data breach means the holder will pay *handsome* compensation out of their data protection insurance (a requirement on Chapters for payment processing as I recall), then perhaps a period of a year might be perfectly reasonable *if* the escrow contract specified the records can only be released as part of a subpoena and the records had to be retained in the country of residence for the person they identify. --Fæ (talk) 23:12, 25 October 2013 (UTC)

sharing info to someone with an nda

The following discussion is closed: ***closing this off for now given the large amount of changes since it was created and the more current discussion about the release to 3rd parties below. Will archive in a couple days unless reopened.***

Perhaps I misumderstand, but I find the following concerning: "*The Wikimedia Foundation will not share submitted materials with third parties, unless such disclosure is (A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department;...*"

Does this mean that the foundation could theoretically give this info to an advertising company provided they signed an nda of some sort? What sort of nda are we talking? As far as I can tell there is no requirement that said nda is a restrictive one, any old nda the foundation legal department likes will do. This seems kind of scary to me.

> Good question, Bawolff. We could say instead: "(A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department **consistent with the privacy policy**". That would limit transfers for uses set out in the privacy policy, which does not include, for example, advertising. If that works for you, we will make this change. Geoffbrigham (talk) 20:04, 1 November 2013 (UTC)

On the subject of passwords, I'd like something a little stronger than that - encrypted with whatever the current best practise is for crypto, with what specific encryption is used. Is there logging? Do different people use different passwords? How many people have access? Is it stored on a non networked computer? (Perhaps the entire security model is out of scope for this document, but I'd like assurances its not just a dummy password with the file on the hard drive being unencrypted. Bawolff (talk) 02:14, 15 October 2013 (UTC)

> Another good question. Our thinking is to have the same level of security that we might use for electronic employee records. But, to be honest, we will need to research this a bit more once we have an idea on how the community would like to proceed. We offered another alternative below where we would not need to store such information. Thanks for your inquiries! Geoffbrigham (talk) 20:15, 1 November 2013 (UTC)

Some food for thought

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active (including too the retention period) I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:22, 3 December 2013 (UTC)***

I'd like to offer some food for thought as to what would personally make me comfortable enough to re-submit my id. This is just my personal idea, and others will have different ideas. I feel the wording of the proposal and the way it has been brought about is very disappointing and a bad start, but I think I understand the underlying reasoning, and agree with it to a certain extent.

I first will seek to explain what is so scary about what's currently in the proposal:

- " Physical copies of submitted materials will be kept in locked cabinets designated for this purpose" -- sorry, if I send you a photocopy of my passport, I'd rather not it be in Philippe's locked cabinet. I want it in an actual, serious safe. And I want to know that only Philippe and Geoff have the combination for it.

  > We are open to different security options, including a safe. But I do want to note that a locked cabinet is the same level of security given to the highly sensitive employee material. What do other community members think about the level of security for physical storage?
  > As for who has access, we can limit the people who can access it, but we should avoid naming specific people rather than offices because this policy (if adopted) should ideally apply regardless of whomever holds Geoff or Philippe's role and take into account what happens if both of them are out of the office. Perhaps something along the lines of "access to these materials will be limited to staff members of the Legal and Community Advocacy department of Wikimedia Foundation"? Mpaulson (WMF) (talk) 21:07, 31 October 2013 (UTC)

- "Electronic copies of submitted materials will be protected by passwords or other electronic protections in files designated for this purpose." This part feels like a bad april fools' joke. I send you a scan of my passport, encrypted with PGP and you just stick it in a zip file with a password that anybody can open with Elcomsoft? Please. If you want to retain electronic copies of our IDs, you need it encrypted, in an offline system and audited by reliable third party firms. And again, only Philippe and Geoff can access it.

  > We intend on giving any personal information submitted or held electronically as a result of this policy draft the same level of security that we give to the personal information of WMF employees or our financial information. Mpaulson (WMF) (talk) 22:17, 31 October 2013 (UTC)

- "The Wikimedia Foundation will not share submitted materials with third parties, unless such disclosure is (A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department; (B) required by law; (C) needed to protect against immediate threat to life or limb; or (D) needed to protect the rights, property, or safety of the Wikimedia Foundation, its employees, or contractors." No, if I send my ID, the WMF can only disclose it following a court order, the end.

  > First, I think it's important to note that there are circumstances that would warrant disclosure that are required by law that would not involve a court order. For example, if we receive a legally valid subpoena or warrant, we would be required to comply with it. (Of course, if we had reason to believe that it was not valid, we would challenge it.) This is why we said "required by law" in subsection (B) as opposed to "compelled by a court order".
  > I'd also like to understand why you are opposed to disclosure if a volunteer threatens immediate harm to another person and identifying information is required by the authorities to prevent such harm (covered by subsection (C)). Could you clarify your position? Similarly, I'd like to better understand your objection to subsection (D), which would allow us to disclose information about a volunteer to proper authorities if they, say, purposefully planted any viruses, malware, worms, Trojan horses, or malicious code that could harm our technical infrastructure in violation of the Terms of Use or that could expose the personal, nonpublic information of other users. Mpaulson (WMF) (talk) 21:43, 31 October 2013 (UTC)

- "Sometimes, the Wikimedia Foundation or a user community committee will need to contact a community member who formerly had access rights about his or her usage of those rights. For example, the Arbitration Committee may need to complete an ongoing case they are examining or the Wikimedia Foundation may need to notify you of receipt of a legal document involving that community member." No, if I give you my address, it cannot be disclosed to some random arbitrator from enwiki because they wish to bring a case against me because I don't fill my edit summaries. It should only be used by the WMF's Counsel, after the WMF has been sued because I disclosed confidential informations that damaged a third party to point the judge to me as the person that should be sued. Nothing else, ever.

  > You may be interested in a related discussion addressing this very issue. Mpaulson (WMF) (talk) 21:13, 31 October 2013 (UTC)

- "For this reason, the Wikimedia Foundation retains submitted materials for a period after the community member ceases to have access rights. Submitted materials will be maintained as long as the community member who submitted the materials has access rights, plus up to an additional three (3) years." You do not need 3 years, so you shouldn't have 3 years. 6 months, sure, 3 years, nope, no way.

> We are open to altering the retention period. Would you mind reading the retention period thread and letting us know what period you think would be reasonable in light of what's written there? (I would really appreciate this as I'm trying to move all comments regarding data retention to that thread so that it's easier to track and easier for everyone to see the considerations involved in determining what the data retention period should be.) Thanks in advance! Mpaulson (WMF) (talk) 23:06, 25 October 2013 (UTC)

- "If a community member ceases to have access rights, he or she should notify the Stewards. The Stewards will inform the Wikimedia Foundation and the submitted materials will be destroyed by the Wikimedia Foundation in a timely manner following the three (3) year period." In no way should us, the Stewards, have anything to do with this stuff. Anything that has to do with IDs or related should be handled by WMF personnel trained in the handling of personal data and on a need to know basis. Said personnel should figure out when it should be deleted, not us.

> Please see Philippe's response on this issue below. Thanks! Mpaulson (WMF) (talk) 22:18, 31 October 2013 (UTC)

- "Community members with access rights may submit the required Identification and Confidentiality materials to the Wikimedia Foundation electronically. Hard copies may be submitted on a case-by-case basis." No, it has been long-standing practice to accept ID in the forms most convenient to the user, and this should not stop. Especially given a locked cabinet is better than a zipped and password protected file, which are the options as it stands.

> We would be fine with that change (assuming that identification documents are submitted at all, a decision that is still pending as we are still waiting to hear more from the community on that matter). Mpaulson (WMF) (talk) 21:56, 31 October 2013 (UTC)

- But above all, there is no reason for the WMF to keep a copy of my passport. Zero. I understand that you need to know who I am and where I live in case you have to sue me, that is okey. But once you saw my passport and established that I am who I am, you only need to keep this information in your archives, you do not need a copy of my id. Be them encrypted offline archives or locked safes.

> Again, we are interested in hearing from more members of the community on this matter. Would the community be more comfortable if we only retained the identification information rather than copies of the identification documents themselves? Mpaulson (WMF) (talk) 21:56, 31 October 2013 (UTC)

- Somebody suggested a bank vault. I actually like that idea. Keep a copy of my name, username and address in a bank vault or if there's a reason why it really can't be there, an outside law firm offices' safe. You don't need anything else.

> We are actually pretty uncomfortable with this possibility. We have some serious concerns about the potential for disclosure if the information is held by third parties. We are pretty vigorous about pushing back on requests for user information when we believe that such requests are not legally valid. We honestly cannot say the same about more traditional institutions such as banks. Mpaulson (WMF) (talk) 21:56, 31 October 2013 (UTC)

I know that there are some folks that cannot live with the IDs being retained, or even their name being retained. I respect them, but that is not my case. I am willing to let the WMF have my name even in perpetuity if they wish. I am not willing to let the WMF keep my passport scan in a zipped file or a locker. I think functionaries deserve more than that, and the wording of this proposal is unacceptable, especially given when this was raised before the OTRS community had grave objections to the locker/cabinet. I know you can't win all of the people over on retaining data, but this attempt is not going to win anybody over period as long as it is construed this way. I am still shocked that anybody at the WMF would be so out of touch to think that a locked cabinet or a password-protected archive was anything but a joke. **Snowolf** How can I help? 02:38, 15 October 2013 (UTC)

> I would like to highlight my experience of the reality of fraud with regard to passports. *Several years ago an Australian friend was looking for an apartment in Paris, knowing his boyfriend rather well, I acted as his UK reference for a money transaction in London for a deposit of more than 1,000 euros for the lady that was looking to re-let her lease. It was a scam and he lost his money (this is now recognized as a 'classic' scam but it was new back then). With the UK police, I investigated the background and key to the scam was a passport scan that had been doing the rounds with scammers for some time. I managed to contact the lady whos passport it was, and she was the victim of an earlier scam and her identity was being used for multiple later crimes, she put me in touch with a fraud detective in Interpol who was tracking all instances of this fraud. Unfortunately once your ID is compromised this way on the internet, it becomes impossible to put the genii back in the bottle, her scanned passport page (with real name and address details) can be still be found on scam websites and is no doubt still being used to commit fraud in her name.*
> +1 for Snowolf's suggestion that **any ID material is not held by the WMF office, but held in escrow** using a service off-site and only accessed after a direct legal requirement to do so, rather than a request from some unpredictable committee of volunteers who are unlikely to be able to prevent emails or material being "leaked" if it turns out to be of interest to the newspapers. These services range from very cheap to free, from banks and legal firms. --Fæ (talk) 08:20, 15 October 2013 (UTC)
>
> - Good idea, however I can imagine also that some community members could feel LESS safe with a third party involved. Pundit (talk) 06:04, 16 October 2013 (UTC)
>
> > We're still working through some of the points that were raised here, but I'd like to respond to a couple of them: first, regarding having the info held by a third party firm - I think that's a bad idea. If we store it in house, my understanding is that we are, broadly, covered by attorney/client privilege for doc here. (Disclaimer, IANAL).

Stewards - It's been raised that the process as laid out here adds work to the stewards (given that they they have to notify us). I can see the point. I suggest that we remove that line, (*edit: it has been removed.*) and staff will monitor the logged actions for what we need. Philippe (WMF) (talk) 21:59, 25 October 2013 (UTC)

> Hi Snowolf. Thank you for your thoughtful comments. We are going to try to address each of your points in turn, in-line. We will get to all of them, but I just wanted to let you know that the responses may come piecemeal because we're trying to address issues throughout the discussion page by subject. Just didn't want you to think that we are only intending to address some of your concerns. Mpaulson (WMF) (talk) 23:01, 25 October 2013 (UTC)

Purpose

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active (including too the retention period) I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:23, 3 December 2013 (UTC)***

This page, nor the wikimedia-l thread, nor the blog post, say anything about exactly what problem this new policy would solve. The current system works well and I see no reason to change it. I think the new one is going to be purely inconvenient for our existing functionaries, mainly per Snowolf.--Jasper Deng (talk) 04:25, 15 October 2013 (UTC)

> I have to agree here. What is the problem with the current system that requires the WMF to give out my address to all and sundry? Chase me ladies, I'm the Cavalry (talk) 13:37, 15 October 2013 (UTC)
> Also, just because other sites might do this doesn't mean we should.--Jasper Deng (talk) 04:54, 16 October 2013 (UTC)
> I agree as well. There is nothing here that solves a problem. All it does is cause new ones. -Djsasso (talk) 16:43, 21 October 2013 (UTC)
>
> > Hi All. You may be interested in reading this post about this very topic. I would be very interested in hearing your thoughts. If you get a chance, please let me know what you think on that discussion thread. Thanks in advance! Mpaulson (WMF) (talk) 22:24, 25 October 2013 (UTC)

Purpose of retention for address

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active (including too the retention period) I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:24, 3 December 2013 (UTC)***

Thanks for publishing this draft and getting us involved. In particular I think it's good that you've not required that the government-issued identification have your address on it, as some countries like the UK do not have an identity card scheme and as I don't drive my only government-issued photo ID is my passport which doesn't have my address printed on it. However, in spite of me applauding this, it does raise a few questions for me.

1. **Verification of provided address**. It seems that with no way of checking the address that the person provides, there is no way of verifying the address that's given. Is this just an accepted risk you're taking?
2. **Purpose of requesting address**. In light of the fact that the information supplied may be completely fictional, I'm not sure what the purpose of requesting it is. Some clarification may be helpful.

--Deskana (talk) 09:35, 15 October 2013 (UTC)

> Some websites, such as couchsurfing, use/used postcards with a code for address verification. If they were accompanied by some wiki merchandise, many users would not mind :) This is apart from the discussion whether an address is actually necessary for the WMF to have. Pundit (talk) 06:02, 16 October 2013 (UTC)
>
> > Hmmm..... interesting Jalexander--WMF 02:42, 19 October 2013 (UTC)
> >
> > > Hi Deskana and Pundit! Indeed, these are some great ideas. I would be interested in your thoughts about the general requirement of submitting an address. Mpaulson (WMF) (talk) 20:53, 31 October 2013 (UTC)

What about stolen accounts?

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active (including too the retention period) I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:43, 3 December 2013 (UTC)***

What will happen if one of these "highly-identified" accounts will be stolen? Just some days ago there was a potential security breach when thousands of hashes has been made almost public on WMF labs. So the owner will be legally charged with every misuse of his stolen account? I use quite strong passwords and secure user-side devices/software but still my account can be forced in every other point of the chain bringing me to WMF. So, from an "investigative" point of view, identification via IP will always be needed, so why do we need to store IDs? You should also be aware of the revolution in security measures WMF must to take since another "labs leak" will expose the Foundation to serious legal threats by her own users so I must presume WMF

will completely re-design their software and their software development process. My bank and other organisation giving me a legally binding online identities signed strong strong agreement assuring me I won't be charged for their faults nor my good faith faults, will WMF do the same? --Vituzzu (talk) 10:58, 15 October 2013 (UTC)

Yes, this is the point I was trying to make, but you put it more clearly :) --**Rschen7754** 04:25, 16 October 2013 (UTC)

@Mpaulson (WMF): are there plans to clarify the wording (I think it was the confidentiality pledge actually)? Personally I would suggest something like "in cases of willful intent to violate privacy, or gross negligence", but IANAL. --**Rschen7754** 20:11, 30 October 2013 (UTC)

Hello @Rschen7754: and @Vituzzu:, thank you for this question. This policy and the Confidentiality agreement for nonpublic information applies to "you" -- the person using the account. Is there another section where this could be clarified? A user should not share his or her password (under the Terms of use), but it is not a violation of these policies if a user's account is stolen (through no fault of the user). In practice, a user will have his or her technical privileges revoked if it appears that his or her account has been compromised. For example, a steward under the CheckUser policy may remove a checkuser's access. The intent is to ensure that checkuser tools are not used by someone who was not selected and entrusted by the community. Thanks Stephen LaPorte (WMF) (talk) 20:15, 1 November 2013 (UTC)

Board of Trustees

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active (including too the retention period) I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:44, 3 December 2013 (UTC)***

I'd like to read some words from the Board about this change. --Vituzzu (talk) 11:12, 15 October 2013 (UTC)

On a similar note, has the Ombudsman Commission taken a stand here on this specific proposal? Pundit (talk) 06:06, 16 October 2013 (UTC)

Hi Vituzzu and Pundit! The Board is, of course, welcome and encouraged to join this discussion. And the Ombudsman Commission actually helped us craft the concepts included in this policy draft and provided useful feedback during the drafting process. Mpaulson (WMF) (talk) 23:17, 17 October 2013 (UTC)

That was my understanding, but I wanted this to be clear. Pundit (talk) 06:57, 18 October 2013 (UTC)

Michelle: it's a bit strange to read that the Board is "welcome and encouraged to join this discussion." This policy has no effect unless the Board says so. The Board is quite a bit more than welcome and encouraged to join the discussion... the Board should be actively leading it. --MZMcBride (talk) 22:32, 20 October 2013 (UTC)

Heh. Surprised? Theo10011 (talk) 23:28, 23 October 2013 (UTC)

MZMZ - A global policy such as this would have to be discussed and approved by the Board to take effect. But that does not mean that all public discussion must be led by the Board. LCA in particular is designed to coordinate public discussions about their work, including any policy recommendations they make to the Board -- such as is happening here. In those cases there are reasons not to have the Board jump in with comments before a public discussion, since the hope is to reach an understanding of appropriate community norms, and we are sometimes derailed by threads that try to oppose board and staff comments [rather than empowering the community to draft a policy it finds appropriate in the first place].
The Board has not revisited this policy since 2007 - see also this comment from 2011 when it was last being reinterpreted. Members of the Board are reviewing these policies and proposals at the same time as the rest of the community, thanks to this public discussion; but we don't get to weigh in "as a Board" until there is a recommendation before us. Which, given the quality of the legal-community discussions in recent years, I am certain will be an excellent one. --SJ talk 19:47, 24 October 2013 (UTC)

Vituzzu - the current policy on how users identify to the WMF, and for what reasons, is vague on how identification is implemented. I do think that this should be covered more clearly in an "access to private data" policy -- at least to be clear about current practice. --SJ talk 20:03, 24 October 2013 (UTC)

Michelle - I appreciate your sentiment. It is hard for Board members to join such a discussion individually, since our primary position in these cases is strong support for staff in engaging directly with the community; and since our personal views are often mistaken for Views of the Board. That said, I have shared some brief personal thoughts below, as a community member and not a Board member, in areas where clarification would help me.

Thank you for clarifying, SJ. Your thoughts are always appreciated! Mpaulson (WMF) (talk) 22:20, 24 October 2013 (UTC)

exact scans vs. data

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active (including too the retention period) I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:45, 3 December 2013 (UTC)***

I understand that WMF may need to be able to link the special trust accounts with actual people. Stewards, checkusers, oversighters have tools which technically allow privacy breaches on all other members of the community and it is only natural, that the safety and privacy of everybody wins with the right to privacy of those tool holders. I'm curious about one thing, though. Several members of the community expressed concern about their ID scans being kept by WMF simply because such IDs, if anything goes wrong, may be used for identity theft. I'm wondering then whether WMF indeed needs full ID scans, or is a basic confirmation of one's identity (with typing a name, date of birth, and possibly a declared or verified address into a database) not a better solution? Pundit (talk) 06:10, 16 October 2013 (UTC)

> If the problem here is that we need a legal record of verification, then I would have far fewer concerns in proving my identity to a local notary public (a solicitor on my high street charged me £5 the last time I did this) and then providing the approved relevant scan to an escrow facility in my country (again, these are cheap as chips or even a free service that the WMF bank or regular solicitors could provide). As for the security of a third party, if it is a bank or a solicitor's secure facility, then the level of insurance/compensation available in case of fraud would be far, far higher and more reliable than the WMF can provide. As a solution this reduces risk of fraud for both volunteers and the WMF, or the catastrophic case where volunteers are being forced to sue the WMF for compensation after a disgruntled employee (or someone else hanging around the WMF not-as-secure-as-a-bank offices) does something stupid. --Fæ (talk) 07:11, 16 October 2013 (UTC)
>
> > (Btw notary public exists only in Common law)
> > Actually I contested the whole process of association between accounts and identities since, from a legal point of view, we cannot give any legal warranty about account strength thus an IP check will always be needed. --Vituzzu (talk) 12:34, 16 October 2013 (UTC)
>
> I don't think we're tied to keeping full IDs. We'll have to think on the option some more, to make sure we're not missing something. Would it reduce your other concerns if we did that? Importantly, would you be OK with us asking for things that might not be on all IDs (such as addresses)? -LVilla (WMF) (talk) 22:49, 25 October 2013 (UTC)

Draft confidentiality agreement

The following discussion is closed: ***close, looks like the discussion is finished/stale, will archive in a couple days unless reopened. Jalexander--WMF 22:36, 9 December 2013 (UTC)***

For the record we have a draft of the agreement mentioned up already which is also available for discussion. Jalexander (talk) 23:07, 3 September 2013 (UTC)

> So just to begin this part of the discussion, the draft of the agreement says the following: *Authorized Wikimedia community members may include, for example, oversighters, checkusers, functionaries, volunteer developers, and other similar authorized roles.* Can we please clarify what exactly is meant by *functionaries*? Also, including OTRS agents in that list might also be helpful. (I'll try to provide more comments as I read through the text.) odder (talk) 21:41, 19 September 2013 (UTC)
>
> > Hi odder! Thank you for your questions and comments! I've responded to each of your inquiries in-line below for the sake of clarity. I hope that's alright.
> > I agree that the term "functionaries" is a little vague. What we were trying to encompass here was any community member who has been given rights that permit them to access nonpublic, legally sensitive information. However, we realize that different communities may have different terms to describe the group I refer to as "checkusers" or may choose to change the term "checkusers" in the future. Similarly, new roles or access rights may be created in the future by the community that should be covered by this policy, but obviously cannot be explicitly listed. We hoped that the general term "functionaries" would suffice, but we are also very much open to other suggestions.
> > I also agree that adding OTRS agents to the list of users covered by this policy might be a good idea considering that people who write to OTRS frequently include sensitive information about themselves or others. What do other community members think about this? Mpaulson (WMF) (talk) 23:21, 15 October 2013 (UTC)
> >
> > > I do think that you would risk a lot of people leaving, and would also put those in between the ages of 16-18 in an awkward position... --**Rschen7754** 00:27, 16 October 2013 (UTC)
> > >
> > > > Hi Michelle, thanks for your answer. I would simply suggest that you remove the word *functionaries* from the draft, as the number of user groups with direct access to non-public, personal and sensitive information is, I believe, very limited; only oversighters, checkusers, stewards and volunteer developers might have access to such information (as well as members of Arbitration Committees on some projects, but they generally hold oversight and/or checkuser rights already). The term *functionaries* is usually supposed to include administrators (and possibly also OTRS agents); you are already using the phrase *and other similar authorized roles*, which, in my feeling, is enough to cover the possible future scenarios you mentioned.
> > > >
> > > > As far as OTRS members are considered, my intention was only to make things more clear to people; if you want to include OTRS agents, then please do so plainly, and we can discuss the pros and cons of the idea afterwards.

> As an OTRS agent, I have seen many e-mails which revealed very sensitive personal information about people, such as exact (snail-mail) addresses and phone numbers, not to mention real names or e-mail addresses. I think I can say I've had access to more sensitive personal information as an OTRS agent than as a Commons oversighter — so I can understand why it might be good to include OTRS agents in the list, and have them sign the agreement. However, as Rschen7754 rightly points out, this idea has always been controversial among OTRS agents, and many of them might decide to leave if this requirement is implemented, so I think we should try to discuss it in detail. odder (talk) 10:15, 16 October 2013 (UTC)
>
> > What do you think about removing "functionaries" and saying "This policy does not require users whose rights only include the ability to view standard deleted revisions."? Mpaulson (WMF) (talk) 22:16, 25 October 2013 (UTC)
> >
> > > Sounds good to me; thanks, Michelle! I'm not sure how to address Bawolff's point about #Volunteer developers which was brought with regards to the privacy policy, but which is also relevant for the confidentiality agreement—any ideas? odder (talk) 07:02, 26 October 2013 (UTC)

So I read the draft, and here are some more questions:

Comply with the Privacy Policy; the Access to Nonpublic Information Policy; and any other applicable and nonconflicting community policy relating to nonpublic information; -- the community policy part is quite vague. Moreover, it is my feeling that it complicates this point a bit by mixing the requirements of the WMF and community policies; on a related note, I'm not aware of any community policies concerning non-public information, nor do I think that it should be up to the community to decide that. odder (talk) 21:58, 19 September 2013 (UTC)

> The reason why we have included any applicable and nonconflicting community policy relating to nonpublic information is because the Privacy Policy and the Access to Nonpublic Information Policy are baseline protections. Nothing in those policies prevent any particular project's community from creating and enforcing more protective policies with regards to user data. If a community does create such a policy, we would expect community members of that particular project who have special access rights to comply with that community's policies. Does that make sense? Mpaulson (WMF) (talk) 23:21, 15 October 2013 (UTC)
>
> > Yes, it does make sense :-) However, we are still left with the question whether the communities should have any say in the subject of protection of user data. So far, this has been a Foundation prerogative, and I wonder if this change would do us any good. (Just throwing a thought.) odder (talk) 10:15, 16 October 2013 (UTC)

The Wikimedia Foundation may pursue available legal remedies. This sounds *very* scary to me, as if the WMF reserved the right to sue me if I violated the agreement. I would very much appreciate a clarification about what's meant by this sentence.

> I can understand why this clause sounds scary. Believe me, I hope that we never, ever have to use it. The scenarios that this clause is meant to cover are extreme...for example, if a particular person who has checkuser rights uses those rights to access and copy personal information about users without any good reason and then goes on to publish that information in a inappropriate or malicious way, we would want the ability to legally restrain this person from continuing to publish the private information. Mpaulson (WMF) (talk) 23:21, 15 October 2013 (UTC)
>
> > Thanks for the clarification, Michelle, it's very helpful. I can definitely understand why you wanted to include this clause in the agreement. odder (talk) 10:15, 16 October 2013 (UTC)

The laws of the State of California and the United States of America will govern this agreement (without reference to conflict of laws principles). This is also very vague; I believe that people should be informed in detail about what applicable laws there are and what are the exact terms that they will agree to if they sign the agreement. (There are many differences between the various jurisdictions our users are located in, and blankly agreeing to be governed by laws you have no idea about is never a good idea, IMHO.) odder (talk) 21:58, 19 September 2013 (UTC)

> Actually, the reason why we have this clause is to clear up ambiguity, not to create more. We want to be clear that a particular set of laws will govern the way this agreement is interpreted (in this case, the laws of CA and the US). But I don't think it's reasonable or even possible to provide every law that could apply to any particular situation that could arise in relation to this agreement. It would frankly turn this 1 page or so agreement into a treatise with many, many volumes. For example, the statutory and case law covering contract interpretation alone could fill the better part of a library. Mpaulson (WMF) (talk) 23:21, 15 October 2013 (UTC)
>
> > Yes, I'm aware of the complexity and the vastness of the U.S. legal code; it wasn't my intention to make you describe any and all laws applicable to this agreement. However, it would still be helpful for many people to know at least the basic terms of the laws they would agree to if they sign the CA. (There are many questions asked about this part by people below, for instance Vituzzu and Fae, so you can see this is something people are actually concerned about.) odder (talk) 10:15, 16 October 2013 (UTC)
> >
> > > Usually there are small differences among the states in the U.S. on issues like construction of the agreement, damages, and consideration (that is, the quid pro quo of contracts). This article

(http://docs.law.gwu.edu/facweb/gmaggs/maggs-augsburg.pdf) points out some differences among different states as well as Europe. It is a bit difficult to be more specific because it will depend on the facts of each case to some degree, and, in a common law country, the case law in the jurisdiction. Geoffbrigham (talk) 22:03, 25 October 2013 (UTC)

> Thanks for the pointer, Geoff; I'm sure the lecture will be interesting, and I'll try to read more on the subject. odder (talk) 07:02, 26 October 2013 (UTC)

Another part of the agreement got my attention today:

> *(...) your activity or account may be reviewed by other authorized users or the Wikimedia Foundation.'* Does anyone mind explaining the meaning behind *your account (...) may be reviewed* and the meaning of *other authorized users*? I'm especially concerned about a combination of these two parts: *your account may be reviewed by other authorized users*. What does this mean with regards to off-wiki activity such as OTRS? Does this mean that in case of a breach of privacy by a checkuser, other community members with these rights would be able to perform a check on their account? I would welcome an explanation of this point, thanks. odder (talk) 17:50, 7 October 2013 (UTC)
>
> > This means that if there is a good reason to suspect that abuse (or mistaken use) has occurred in relation to a particular account with access rights, the Foundation or other community members with the same rights may review the account and its activity to ensure it is in compliance with applicable policies and that nothing has gone wrong. To be honest, it is unlikely that the Foundation would play this kind of role unless the alleged abuse in question was significant. The more likely scenario is that something unusual happens (or something usual happens and was incorrectly documented) and the other users with the same access rights proceed under their own policies to investigate the matter. Mpaulson (WMF) (talk) 23:21, 15 October 2013 (UTC)
> >
> > > So, to take your example from above, I'm assuming that in case of a checkuser revealing non-public information about another user off-wiki, other checkusers will be able to perform a check on them — is that right? I'm not exactly sure if volunteer community members should be tasked with ensuring compliance with Foundation's policies in cases like that. Also, I'm assuming that in case of OTRS, it will be the OTRS admins ensuring compliance with the various policies (please correct me if I'm wrong). In any case, thanks so much for your answers, Michelle; I appreciate your time. odder (talk) 10:15, 16 October 2013 (UTC)
> > >
> > > > The intention here - as I understand it - is to say that nobody gets to do unreviewed actions. Not Checkusers, not oversighters, and not me. It's a bad idea to have a system where anyone can pull data without creating an opportunity for review of the action. That's why we have logs that are automatically created... my read of this sentence is to spell out clearly that if you Checkuser someone, you should expect that the Checkuser logs will be reviewed. Likewise, if you're oversighting, you should expect that those logs are reviewed. That applies to WMF staff too - I review the logs for staff names, and I know that (for instance) when the English Wikipedia sees a staff member do a checkuser who isn't typical, they review it and notify me. So I interpret the sentence to mean that the actions of the accounts may be reviewed (and, as well, other data about the account (ie, was it logged on then?) if needed. Philippe (WMF) (talk) 21:48, 25 October 2013 (UTC)

OTRS volunteers

The following discussion is closed.

The draft is not very clear about identification requirements for regular OTRS volunteers. For some time now (despite many didn't like it), every OTRS volunteer is supposed to be identified, but in practice past volunteers (and perhaps some of the new too) were not asked to provide identification. Is some clarification of the issue coming? --Nemo 06:13, 4 September 2013 (UTC)

> Agreed imo. Age restriction for OTRS volunteers is set to 16 currently. In my opinion, OTRS volunteers who do not reached at age 18 should be marked seperately in Identification noticeboard. – Kwj2772 (msg) 08:22, 4 September 2013 (UTC)
>
> > That fairly clearly marks someone as "under 18", doesn't it, potentially opening us up to disclosure and child protection issues? Philippe (WMF) (talk) 10:07, 4 September 2013 (UTC)
> >
> > > Then raising the age restriction to 18 would be only option if we're really going to go identification process for OTRS volunteers. Otherwise we can't distinguish them from the identification for checkusers/oversighters. – Kwj2772 (msg) 10:28, 4 September 2013 (UTC)
> > >
> > > > Couldn't we, though? We just have to do it in a more secure area. For instance, we could use a message board that stewards have access to but others don't. Philippe (WMF) (talk) 10:35, 4 September 2013 (UTC)
> > >
> > > Child protection issues for OTRS volunteers?? I might have lost track of what "child protection" term is used for in USA, can you explain? Anyway, whatever you decide please make clear decisions and apply them or it will be again a huge mess with flames everywhere and mass sacrifices of innocents. --Nemo 21:02, 4 September 2013 (UTC)

> > If an OTRS volunteer is under 18, they deserve the same protection that we offer anyone else. :) Philippe (WMF) (talk) 21:56, 4 September 2013 (UTC)
> >
> > > That is? I just said I've no idea what protection you're talking about... --Nemo 12:29, 5 September 2013 (UTC)
> > >
> > > > Sounds like protection from revealing personal information, which would happen if you put someone's name in a section which specifies that they are younger than 18 but older than 16. Philippe's logic is definitely sound here, but I wonder if the OTRS age should be raise to 18 for consistency and to address the issues raised. Ajraddatz (Talk) 19:07, 14 October 2013 (UTC)

We have been talking internally about whether OTRS agents should be covered by this policy. Currently, only OTRS administrators are covered. There are strong reasons to consider adding OTRS agents given that they have access to nonpublic emails sent by third parties which frequently include sensitive information about those who sent the email (and others). I understand that the current minimum age for OTRS agents is 16. If we were to add them to this policy, we could either make the minimum age 16 for OTRS agents only and keep the rest at 18 or the OTRS agent minimum age could be raised to 18. What do others think about these ideas? We've love to hear the community's thoughts on this subject. Mpaulson (WMF) (talk) 23:28, 15 October 2013 (UTC)

> If you raise the age to 18, then there arises the issue of what to do with those who are between 16 and 18. Any account removals would be publicly logged, and people could guess their age that way. --**Rschen7754** 02:41, 16 October 2013 (UTC)
>
> > Fascinating point! If the age is raised, then removing <18 accounts would clearly identify those users as such. However, you couldn't simply grandfather them in - why would the change be needed in the first place if current 16 year olds still had access? Ajraddatz (Talk) 02:54, 16 October 2013 (UTC)
> >
> > > The OTRS admins could simply not remove people <18 from the public list of accounts immediately, but at later times in smaller inconspicuous groups (to make it look like normal fluctuation). --MF-W 14:12, 16 October 2013 (UTC)
> > >
> > > > Now that you've said that, it's probably not going to be a useful way to hide it. You could just get rid of all non-identified OTRS agents with the same reason, not making public whether it was over their legal ability to usefully identify or not. --Krenair (talk • contribs) 23:53, 20 October 2013 (UTC)
> >
> > If having <18 people hasn't caused any issues for this long, there won't be any issues for two more years. We could just stop accepting new applications from people under 18, and then people who are currently under 18 will be 18 within two years. -- King of ♥ ♦ ♣ ♠ 23:21, 25 October 2013 (UTC)

> Regardless of whether OTRS users should be subjected to this outrageous policy, the thing with the Identification noticeboard needs to be clarified. It is untenable that someone might identify for OTRS, be added to the I.N. and then happen to become a CU/OS/steward based on that entry, even though he is still <18. --MF-W 14:12, 16 October 2013 (UTC)
>
> > Yes, but admin actions are generally logged on OTRSwiki. --**Rschen7754** 17:29, 16 October 2013 (UTC)

Speaking as an OTRS volunteer, I have no problem with being identified to this degree - David Gerard (talk) 22:26, 25 October 2013 (UTC)

> Doesn't bother me, either. The age issue is interesting, two questions: (1) how many would this affect as of today and (2) is this to do with the age of legal majority and legal responsibility for handling this kind of informaiton (probably covered already but there's a loooot to read through). JzG (talk) 22:54, 25 October 2013 (UTC)

As an OTRS volunteer, I think it would be even necessary to identify yourself, because there are some volunteers that would have probably have much more professional and warm approach to people addressing OTRS, if they weren't allowed to hide behind pseudonyms. And as someone, who became an admin on a local Wikipedia at the age of 14, I don't really think age is a good measure when it comes to someone's maturity, responsibility, loyalty to community or ability of taking autonomous decisions, but in this case it would probably make sense to restrict it to 18 for legal reasons. Of course, the information should stay of a closed nature (at least I don't want that just about everybody has an access to a photocopy of my id and would definitely reconsider my volunteering if any of these data date would become public) --Smihael (talk) 23:48, 25 October 2013 (UTC)

> I don't have a problem as well with such identification. I am not sure about the legal issues, but if this wasn't severely needed, I would highly oppose such a restriction. Many of the active Wikimedia contributors are school students, and a lot of them become admins before 18. Possibly many of the OTRS agents, too. The important thing is, how far is this necessary; was there any particular case ever when this caused a serious problem? In the case there wasn't, how much would be the possibility of having such a problem in the future? And what's its worst possible scenario for it? I would like to know what the answers looks like before making an opinion --Abbad (talk) 04:53, 26 October 2013 (UTC).
>
> > As volunteer i don't any problem with my identification using a regular system (CU, OS, ...). Alan (talk) 15:16, 26 October 2013 (UTC)

> How about no. I gave my real name and my emailadress. This should be enough. I don't see why people have to send ID's. My privacy is worth more than beiing an OTRS-member which I quite enjoy. Some things are private. Why do they want to know what I look like? Why do they want to know where I live? --Natuur12 (talk) 21:02, 26 October 2013 (UTC)

I just wanted to note something, from a personal PoV (although I am an OTRS Admin I am speaking only on behalf of myself). Ever since May 1, 2007 (https://meta.wikimedia.org/w/index.php?title=OTRS/Volunteering&diff=next&oldid=575099), it has been clearly stated on the OTRS Volunteer application page (although over the years there have been minor tweaks to the wording), that applicants *must* be **willing** to provide identification. The current wording is "Before applying, please ensure that you are...Willing to provide identification to the Wikimedia Foundation if necessary, considering the access to nonpublic data policy". *So this really should not be such an issue for OTRS Agents*. Putting that aside, please remember that the current drafted version, and the drafts we've gotten all along up to this point have never included OTRS Agents under the policy; only Administrators will be affected. Rjd0060 (talk) 01:11, 27 October 2013 (UTC)

> Thus far "providing identification" has only ever meant that copies of the identification would *not* be retained (something that has been reiterated a number of times since 2007), so I'm afraid I don't see the link. **Thehelpfulone** 01:38, 27 October 2013 (UTC)

> > There are users that are concerned with providing the ID all together, before even considering the fact that the information will be retained. But again, the most important thing here ... it isn't set to apply to Agents. Just the Admins. Rjd0060 (talk) 01:44, 27 October 2013 (UTC)

> > > What do you folks think about WMF eliminating the identification process and leaving it to the community to come up with their own standards of identification (consistent with the privacy policy)? I have heard so much objection to identification itself or the various proposed means of identification, so I'm interested in your views to this proposal. Identification without retaining the identifying information is not consistent with the spirit of the Board resolution in my opinion ("Only persons *whose identity is known* to the Wikimedia Foundation shall be permitted to have access to any nonpublic data or other nonpublic information....") So I'm honestly thinking of asking the Board to revoke its resolution and leave to the communities to put into place identification processes that work for their specific communities and needs. Thanks for your thoughts. Geoffbrigham (talk) 22:45, 15 November 2013 (UTC)

Balancing WMF's need to protect itself with volunteers' need to protect themselves

I am an OTRS volunteer. Through OTRS I was given access to (i.e. I handled as part of normal OTRS activities) an email in which I was pointed to a file that had enough information easily steal two people's identities. Obviously the file has since been Oversighted.

In order to get access to OTRS I sent a WMF staff member a copy of a state-issued ID, with some information (anything they didn't explicitly ask for) blurred out, with the understanding that the image would be deleted as soon is it was looked at.

I can absolutely understand the WMF's desire to have a better grip on who is handling the sensitive information on WMF projects. While it's certainly not every day that someone uploads a large chunk of personally identifying information to Commons, it's not entirely uncommon either. But it's important to note that all being an OTRS volunteer did was *point me at the file*. The file was already publicly available, and could have been found just as easily by ordinary Commons users doing cleanup (considering that the uploader had a serious misunderstanding of what Commons was, the file was likely uncategorized, and thus someone else finding it while doing cleanup is a near certainty). Hell, it could just as easily have been found by some random editor clicking 'Random file'.

The vast majority of the sensitive information that OTRS volunteers have access to is phone numbers and email addresses. Celebrities generally have paid staff dealing with OTRS on their behalf, so it's really just the phone numbers and email addresses of random, generally unremarkable (no insult intended) people.

The policy, as written, is unpalatable to a majority of the users that are participating in the discussion. That could be because a lot of people read the and policy and did commented because they have no issues, but considering that there are almost no positive messages about the policy, I would have to say that seems unlikely. On the contrary, right now several functionaries that would be effected by the new policy should it go into effect are threatening to resign over several clauses (parts 3.(b) and 3.(d) mostly).

OTRS already has backlogs that come and go based largely on the availability of volunteers, and it needs a large body of people to keep things running smoothly. If this policy is extended to all OTRS members, some of them *will* resign. I personally will, (and although I'm not active now, at one time I was doing a majority of the photosubmissions queue work). I have to imagine that other people will as well. If too many people decide that they're not going to accept the new policy, it leaves OTRS in a weaker position in terms of timeliness of responses, but does it really lead to a stronger position in terms of security? Is there really any positives? Do we really need to have the names and addresses of OTRS volunteers? I don't think so.

The WMF needs to balance the need to protect the WMF with volunteers' need to protect themselves. The WMF wants to have this information on file in case something goes horribly wrong and it becomes a legal issue, either where the WMF has to declare that personal information it was handling was leaked, or where someone writing into OTRS brings legal action (legitimate or no) against the person that responded to them.

However, by the same token, individual users have to protect themselves. Looking at the Wikivoyage fork debacle, one wonders if more people would be parties to that (frivilous) lawsuit if more people's information was public. If the WMF *doesn't have* the names and addresses of volunteers, it can't *give people* that information. That gives volunteers an added layer of protection from, to put it tactfully, are *unpleasant*. If volunteers don't feel that they have that layer of protection, they're not going to be willing to handle the angry people that write in threatening to sue the WMF and everyone that edited some article or another, and they're not going to be willing to handle the people that seem of questionable grounding.

Ultimately, I don't feel that there is enough of a benefit to the WMF, or enough of a risk that the WMF needs to protect against, to warrant having OTRS volunteers as an included body for this policy. Sven Manguard (talk) 20:42, 31 October 2013 (UTC)

> Thanks Sven Manguard. What do you think of our proposal to eliminate the identification process? Geoffbrigham (talk) 00:55, 6 November 2013 (UTC)

- **Note:** Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 18:49, 9 December 2013 (UTC)

Signing the pledge and resulting liability implications

The following discussion is closed: ****Note: Given how the changes made closing this has done, will archive in a couple days unless reopened. Jalexander--WMF 19:12, 9 December 2013 (UTC)***

Having trusted users sign a pledge in association with their full legal identity, appears to be an enforceable contract between the legally identified person and the Wikimedia Foundation. This would appear to make the trusted user liable for damages in a case raised against the WMF for any actions the trusted user may have been involved with, or thought to be involved with, whether they were paid for their time or not. Three questions:

1. By signing this contract, exactly what potential liability does the trusted user take on for the consequences of their actions and is the liability limited or unlimited?

2. Would the WMF be obliged to provide legal identities for trusted users so that a complainant could name them in a legal case of damages?

3. If there is a risk of liability, will the WMF provide liability insurance that will be sufficient to cover expenses or damage claims in any future legal action with respect to any actions a volunteer might have made as a trusted user? I note that in the UK, such insurance is commonplace for charities where volunteers may take on operational duties as well as employees. Wikimedia UK gives its volunteers this form of liability insurance when acting for the charity, and the volunteers have access to the policy to review if they wish.

--Fæ (talk) 23:55, 14 October 2013 (UTC)

> I'm not a lawyer, but I think the question of whether its enforceable or not (and to what extent) is not super settled. I'm sure there is a category of law out there dealing with "contracts" with unpaid volunteers, but I think generally speaking for an agreement to be binding there needs to be a degree of consideration involved. It's a similar issue as applies to non-disclosure agreements between entities where the NDA is the only tie. In this case, the information probably has no commercial value either, so... the agreements are basically a promise to tie you up in court and cost you money with legal fees, that's about it - and even *that* is only for parties within the U.S. Good luck enforcing a non-disclosure agreement against a checkuser in Russia or Italy or China. (edit to add: in other words, its all paper covering the WMF's ass and not much more.) Nathan T 00:11, 15 October 2013 (UTC)
>
> > I can understand your concerns, but I'm comfortable with the language of the agreement for our purposes. Consideration usually needs to be only minimal, and frankly resort to enforceability would only be reserved for really exceptional cases; our primary objective is to spell out the clear expectations of the community in the handling of non-public user information, so people comprehend their responsibilities. Courts may limit liability according to the circumstances, but I would imagine that the most common legal remedy would be a declarative judgment to comply with the agreement or injunctive relief not to disclose further private information. I don't understand the question about "legal identities." WMF may be required to disclose information in its possession if it received a legally-valid subpoena consistent with the privacy policy - though we aggressively resist subpoenas that are overly broad or otherwise legally deficient. As a matter of practice, we also notify users when possible relating to subpoenas requesting their user information. See draft privacy policy. Since the volunteers in the community do not act on behalf of WMF, we would not provide insurance, though we do have available for administrators the Legal Fees Assistance Program when applicable. Also we have suggested an alternative approach below that addresses some of the concerns you mention here. Take care. Geoffbrigham (talk) 19:53, 1 November 2013 (UTC)
> >
> > > @Geoffbrigham: Well, the problem is that a lot of volunteers are not comfortable with the language. Our signing this pledge would basically give our legally binding consent for the WMF to file a suit against us for damages. I've interacted with enough WMFers to know that you would only pursue legal action when necessary; however, we don't know who the WMF will hire down the road, and we would hate to be wrong about something like this. Adding additional language to clarify the scenarios in which WMF would file a suit would go a long way. Speaking for myself, this is the dealbreaker for me - I might not be happy about the rest of it, but I might go along with it anyway; yet the liability issue and my possibly having to take out insurance just to be a steward/CU/OS or whatever is problematic. --**Rschen7754** 20:17, 1 November 2013 (UTC)
> > >
> > > > Thanks for the clarifications Geoff. I take from your statement that:

1. Despite insurance being mentioned elsewhere on this talk page, the WMF does not actually insure any volunteers or other trusted users and has no intention of doing so, even where WMF projects rely on these volunteered services. I note that some Chapters do insure volunteers when acting in roles that would otherwise have to happen through paid project contractors, and this does happen as standard good practice for a large proportion of other charities that rely on volunteers to deliver charitable services to their beneficiaries.
2. You understand my concerns, but you remain comfortable with the policy as it fits your purposes.
3. The legal document has the primary objective of spelling out expectations for handing non-public user information. That it now creates a mechanism for legal enforcement, such as a volunteer being sued by the WMF for indefinite sums of money, seems a secondary concern.
4. The WMF shall pass on legal identities of volunteers in response to any valid subpoena from any party.

--Fæ (talk) 23:34, 1 November 2013 (UTC)

> Hi Rschen - so I guess I need to understand better what you think is acceptable. As we suggested above, we could create a regime without identification, which would alleviate some of the above concerns. If that is not the approach that the community wants, we could try to limit the type of legal relief - such as a restriction to injunctive relief. Or we could allow monetary damages up to a certain amount ($30,000?) or only with a significant level of legal intent (something like "willful" disclosure). The challenge is that we cannot anticipate all situations. The one "test" question I ask myself is if a checkuser sells nonpublic information for personal profit, what remedies would the community find appropriate? I would be most interested in your thoughts on this. Thanks. Geoffbrigham (talk) 08:55, 6 November 2013 (UTC)
>
> > "Willful disclosure" would be fine by me, or "gross negligence" (choosing a password like "password" for example, or allowing someone to borrow your steward account and that person does bad things with it, etc... when the holder of the advanced rights clearly should know better - though I can see how that might be a harder line to draw). I personally don't see the same issues with injunctive relief, since at least according to my understanding, any financial impact would be minimal (as long as you don't break the agreement). I don't think many people would have problems with the WMF asking for monetary damages if someone with access to public data purposefully violated someone's privacy to the extent that it caused them real-life consequences (though the case could be made for the person who was outed suing too...) --**Rschen7754** 09:13, 6 November 2013 (UTC)
> >
> > > Rschen - You are correct that injunctive relief would be limited to an order to stop doing something (like "stop your access to and distribution of nonpublic information") - without monetary damage awards. We could limit monetary damages to "gross negligence and willful disclosure." It would mean that a volunteer acting negligently with real consequences to the privacy of others would not pay monetary damages pursuant to the agreement. Does that work for you (and others)? Geoffbrigham (talk) 23:59, 6 November 2013 (UTC)
> > >
> > > > Hi Geoff, you have used some words that I find difficult to interpret, both due to my past professional experience and probably because I am reading them with a UK understanding of English whilst you are writing them from a USA standard. To be honest I worry that many readers here might jump to incorrect interpretations of the specific legal words you are using and so their feedback might end up being based on unwarranted assumptions.
> > > > Putting aside "willful disclosure" (though I think that needs specifying), my understanding of a statement that the WMF will *"limit future claims of damages against volunteers to cases of gross negligence"* is linguistically and legally equivalent to the WMF will *"be free to claim (unlimited) damages against any volunteer where there are allegations of them behaving carelessly"*. It might help our understanding if you could explain your understanding of the specific scenarios that "gross negligence" or carelessness can apply to, in the context of Wikimedia volunteer activities, in plain English, that volunteers can then use as a reference to go back to, in the unlikely event of this becoming a reality. My apologies if I am misunderstanding your intended meanings here, though if I am having difficulty, I am certain others are too. Thanks --Fæ (talk) 00:21, 7 November 2013 (UTC)
> > > > I guess I'm not sure what the difference between "gross negligence" and "negligence" is - is there an accepted legal definition? Other than that, I personally am fine with it. --**Rschen7754** 00:36, 7 November 2013 (UTC)
> > >
> > > Good question Rschen. The difference between negligence and gross negligence will depend on the facts and the duty of care that someone exercises. Some helpful references are here on negligence and gross negligence. Geoffbrigham (talk) 01:10, 7 November 2013 (UTC)
> >
> > Thanks for the clarification Geoff. The English Wikipedia article you provide for a legal definition appears to show that the difference between negligence and gross negligence is a matter of debate and as clear as mud. I suggest if the WMF

wishes to have a legally enforceable policy and if anything goes wrong in the future it can be shown that volunteers accused of carelessness were clearly advised of the policy/pledge and its consequences in a way they could be judged to understand, then the WMF will have to define these terms in specific and appropriate ways that us volunteers do understand.
For example, as a Wikimedia OTRS volunteer the WMF has now stated that I have no legal protection or insurance, effectively if anything goes wrong then my house is at risk. If I agree to the pledge, does this mean that the WMF will help those that wish to sue me or that the WMF will sue me for damages themselves, say for carelessly pressing the send button on an email thread with personal or legal information in it, after putting in the wrong email address?
It would be really nice if at some point the WMF were to turn this around and put our minds to rest by offering liability insurance for unpaid volunteers that were taking on these functions for Wikimedia, in the same way employees were protected. This already happens in Chapters and other charities, it seems odd that the WMF is resisting this solution. --Fæ (talk) 09:11, 7 November 2013 (UTC)

> @Geoffbrigham: Having thought on this, I do wonder if adding "gross negligence" is opening up a can of worms, and maybe it should be left as "willful intent". "Willful intent" seems to be closer to the practice that I have heard from another staff member, as to their thoughts when they would pursue legal action (for extreme cases of someone revealing massive amounts of personal information). --**Rschen7754** 10:53, 15 November 2013 (UTC)
>
> > Hi Rschen7754 - Let's see what others say, but personally I'm fine with limiting statuary damages to acts of willful intent. Geoffbrigham (talk) 01:26, 16 November 2013 (UTC)
> >
> > > Hi Geoff, I am glad to see some movement on the odd word. A pity that the larger direct questions are seen to go unanswered. --Fæ (talk) 03:48, 16 November 2013 (UTC)

Bump. --**Rschen7754** 20:58, 3 December 2013 (UTC)

> Just a note that I've poked the lawyers for this thread. Jalexander--WMF 21:10, 3 December 2013 (UTC)
>
> > OK ... let's limit it to willful intent, given no other responses here. I will ask James to make the change. Geoffbrigham (talk) 21:36, 3 December 2013 (UTC)

Consideration of feedback given over the past week

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 19:13, 9 December 2013 (UTC)***

I would like to thank all of you who have provided very thoughtful feedback on this policy draft over the past week. Your suggestions and questions are much appreciated and have given us a lot to think about. We are internally discussing and brainstorming about many of the issues you have raised and I hope to provide more detailed responses and alternative suggestions over the next week. We may not get to everyone's comments as quickly as we hope to, but please be assured that we are reading and thinking about what each of you say in this discussion and will respond as best as we are able. Thank you again for taking the time to help shape and improve this policy draft. We sincerely hope that with the input we receive over the next few months, we will be able to craft a policy that reflects community values and adequately protects the privacy of both the community members who are in the valuable roles affected by this policy as well as the users whose nonpublic information they handle. Mpaulson (WMF) (talk) 17:24, 20 October 2013 (UTC)

Affected users who will resign if the policy is implemented in its current shape

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. It seems if we're going to have a list like this it should start anew given the large changes. Jalexander--WMF 19:19, 9 December 2013 (UTC)***

(this one (https://meta.wikimedia.org/w/index.php?title=Access_to_nonpublic_information_policy&oldid=6088605), where only non-central feedback was yet taken into consideration)

1. MF-W (steward, OTRS access) 22:04, 20 October 2013 (UTC)

> I haven't had time to read through your comments above quite yet, but it seems strange that nobody is editing the proposed policy to make it acceptable. It's a draft. Be bold! --MZMcBride (talk) 22:34, 20 October 2013 (UTC)
>
> > I think one of the main issues is that there is no specified/apparent reason for this change. It's a solution looking for a problem. It doesn't make sense to try and fix parts of it when the reason behind the entire thing is one of the biggest issues. Ajraddatz (Talk) 22:52, 20 October 2013 (UTC)
> >
> > > Do you agree with having wmf:access to nonpublic information policy? --MZMcBride (talk) 02:01, 21 October 2013 (UTC)
> > >
> > > > Your reply addresses nothing of what I said. I agreed to that policy when I identified to the foundation. You'll notice that I specify the need for change which is lacking, not the need for the policy in the first place. Ajraddatz (Talk) 02:11, 21 October 2013 (UTC)

> Sorry, when you said "it's a solution looking for a problem," I thought you might mean having this policy was a solution looking for a problem, not updating it. I've attempted a better system of discussion below, though I understand that you feel a rewrite is entirely unnecessary. --MZMcBride (talk) 02:54, 21 October 2013 (UTC)
>
> > Ah. Sorry for my hostile response too, I assumed bad faith and thought you were trying to lead my logic to somewhere that I didn't want it to go. I've been studying Plato's works too much recently :/ Ajraddatz (Talk) 03:18, 21 October 2013 (UTC)

2. Trijnstel$_{talk}$ (steward, CU commons, CU meta, OTRS access) 22:17, 20 October 2013 (UTC) Unless some major changes are made ... otherwise I'm not sure I would stay.

> What kind of major changes? --MZMcBride (talk) 22:34, 20 October 2013 (UTC)
>
> > I do not wish to re-identify so that the WMF can keep my ID. That change should be reverted (among others). Trijnstel$_{talk}$ 16:15, 21 October 2013 (UTC)

3. **Rschen7754** 22:28, 20 October 2013 (UTC) (Wikidata oversighter, OTRS access) Only because I have no money to give to the WMF if they sue me for an honest mistake.

> Noting that if the proposal as written passed as of this timestamp, I would be able to fulfill the requirements. --**Rschen7754** 10:47, 4 December 2013 (UTC)

4. Vituzzu (talk) (steward, OTRS access, meta checkuser) it should completely rewritten following a bottom-up process. 22:35, 20 October 2013 (UTC)
5. User:Nillerdk (OTRS access): I will not accept WMF to give away my ID to any third party, not even if required by US law. I will thus not give WMF in USA my personal informations under any circumstances. I *would* give personal informations to my local chapter, but I would only allow them to share my ID with third parties if required by national low in my country. Nillerdk (talk) 15:55, 21 October 2013 (UTC)
6. -**Barras talk** (steward, meta CU, meta OS, simpleWP OS, simpleWP CU, OTRS, CU-I admin if that matters, and while I'm on it probably just all rights straight away as protest, which includes several admin and crat rights along with my duties as GC for both groups, wikimedia/wikipedia and cvn) - As I'm not allowed by German law to re-identify under the condition, that WMF retains a copy of my ID card. See German laws §§14-20 PAuswG. I won't break German law to fulfill some weird rule here. -**Barras talk** 15:57, 21 October 2013 (UTC)
7. I probably would as well. I don't need these rights. So subjecting myself to such a potentially damaging situation is probably not in my future. -Djsasso (talk) 17:05, 21 October 2013 (UTC)
8. DaB. (talk) (OTRS-access, dewp-ml-admin, Toolserver-admin (until end of year) and I'm sure some more). The WMF is not able to protect such simple things as email-addresses or password-hashes, so I can not trust them with something as valuable as my passport. That the US is a 3th world-country in terms of Datenschutz is another problem. And finally I'm not allowed by German law to make a copy and give it to the WMF. --DaB. (talk) 19:21, 21 October 2013 (UTC)
9. Should the policy be adopted in its current state, I would have no choice but to let my identification lapse and hence be removed as steward and enwiki oversighter. While I truly enjoy the work we do here, and would love to keep doing it, the policy as it's worded is not acceptable, it's amateurish and it's stupid. It shows how little somebody at the WMF cares about our personal info, and does not make me sure enough that my information will be safe. I am more than willing to accept some compromise, but this is a scorched earth policy and it hurts me to see the WMF take this approach. We are volunteers, we built this projects or helped maintain them, we don't deserve to be treated like this. **Snowolf** How can I help? 16:57, 22 October 2013 (UTC)
10. The WMF can not be trusted bacause it is based in the US. It's that simple and I will resign my OTRS-access as soon as I am prompted to send a copy of my ID card. --McZusatz (talk) 14:53, 24 October 2013 (UTC)
11. --Natuur12 (talk) 21:10, 26 October 2013 (UTC) I will quite as an OTRS-voluntere if this policy becomes real.

Hi All. First, I would like to note that nothing in this policy draft is settled. The draft is just that...a draft. Anything contained within it is up for debate and suggestions. Second, we would really like to hear your thoughts on the discussion below about whether an identification policy is still needed. Thank you all in advance for your feedback. Mpaulson (WMF) (talk) 22:39, 24 October 2013 (UTC)

Volunteer developers

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 19:20, 9 December 2013 (UTC)***

There are some very weird ideas that a lot of people appear to hold about what/who the developers are. Some people think that we're all paid WMF staff. Others think that we're all system administrators. Those that think we're all system administrators probably think that we can all see nonpublic information. This document arguably makes that assumption or implication in a couple of places:

> "The following conditions are minimum requirements that all community members, including volunteer developers, must meet to qualify as a candidate."
> "All community members who are granted access to nonpublic information rights ("access rights"), except volunteer developers, are typically chosen by the community"

Volunteer developers are not automatically granted access to any nonpublic information. It's unclear to me whether or not this policy could cause any issues, but still... --Krenair (talk • contribs) 22:43, 20 October 2013 (UTC)

> A fine point, Krenair. "Volunteer sysadmins and others with access to shared databases" might be more appropriate here. –SJ talk 19:40, 24 October 2013 (UTC)
>
> > Hi Krenair and SJ! This policy draft was meant to only cover volunteer developers who do have access to nonpublic information, not every volunteer developer. SJ, is there any risk with your suggested wording that it would inadvertently cover developers who only have access to shared databases that do not include nonpublic information? Mpaulson (WMF) (talk) 22:45, 24 October 2013 (UTC)

The language you use the first time it comes up in this document is good. –SJ talk 05:13, 25 October 2013 (UTC)

Policy should be rejected!

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 19:22, 9 December 2013 (UTC)***

This is far beyond what is actually needed for the Wikimedia movement. I am feeling very uncomfortable if the WMF even thinks about this too far going proposal. After all the NSA/etc scandals this is what they come up with?? Sorry, absolutely no. In the whole text I see no reasonable explanation why extra requirements for identification are needed. A lot of bla bla but no actual reason why there is an actual need for. "*Because we believe that safeguarding the privacy of the Wikimedia community is an important Wikimedia value,*" -> if WMF is really thinking that, they wouldn't have proposed this policy that asks too much of giving up the privacy of volunteers. Romaine (talk) 01:12, 21 October 2013 (UTC)

Identity fraud is one of the most intrusive things people can experience. Identity fraud starts often with people knowing the birth date, as that information is often used for organisations to identify someone over the fone (etc). The WMF has no reason at all to keep copies/scans of an ID card. The government in the Netherlands forbids making copies/scans of IDs and also highly recommends not to disclose any information on the ID cards to unauthorized people. WMF is in the private sector and is not authorized to ask for this. Romaine (talk) 01:42, 29 October 2013 (UTC)

Hi Romaine. I just wanted to make sure you saw the more detailed reasoning laid out in the discussion below. I also wanted to make it clear that we are very open to alternate ideas about how community members with access rights identify to WMF and are interested in hearing your ideas. Mpaulson (WMF) (talk) 18:34, 31 October 2013 (UTC)

Attempt at a better evaluation of this draft

The following discussion is closed: ***Closing this whole section because it's all based on the old draft, including the quotes etc, and there hasn't been much response on it for a while partially because of that. Will archive in a couple days unless there is a reason to keep it open. Jalexander--WMF 20:14, 9 December 2013 (UTC)***

I'm going to try subsections and a cute template ({{talk page section}}) to evaluate each section of this proposed rewrite to wmf:Access to nonpublic data policy. I'm going to try to do this in a logical order. --MZMcBride (talk) 02:47, 21 October 2013 (UTC)

I am having difficulty of understanding the value of eating up volunteer time to create a detailed section by section or word by word review, when fundamental questions such as why this policy is needed, what the legal impact on unpaid volunteers is going to be and who will be given access to critical legal records of identity, have yet to be answered. The detailed text of the policy draft is likely to be significantly changed or have different assumptions underpinning it before these questions are resolved. Thanks --Fæ (talk) 13:06, 21 October 2013 (UTC)

The very first subsection covers the "why this policy is needed" needed question, doesn't it? Part of finding consensus is identifying areas of disagreement. We currently have a similar policy passed by the Board in 2007. Do you disagree with having this policy? If not, we should then discuss the proposed rewrite. If nobody agrees with any of the sections of the proposed rewrite, it'll be fairly trivial to reject the entire rewrite outright, right? --MZMcBride (talk) 13:17, 21 October 2013 (UTC)

No, it does not, this was raised earlier on this page and is still awaiting an answer. You cannot start a detailed document review, paragraph by paragraph, until the underpinning reasons for why the document exists and what impact enforcing it will have, is addressed. As to whether I disagree with this document or not may actually be irrelevant, the WMF are not legally bound to respect a community consensus here, and unless I missed it somewhere, I do not think they have stated anywhere that they shall respect a consensus as a management choice. --Fæ (talk) 13:40, 21 October 2013 (UTC)

+1. It certainly makes sense to write down comments section by section or piece by criticized piece, but this has already been done above by some users, see e.g. #Some food for thought by Snowolf. Comments are piling up on this page for about a week now, in which people protest against all sorts of sentences which they perceive as very objectionable in the draft. Meanwhile the Foundation hardly reacts. It is nice to read in #Consideration of feedback given over the past week that WMF discusses what we write and will at some time maybe react (hahaha), and that M. Paulson has even been answering here while being sick (which is, no doubt, sth. we can be grateful for), but afaik WMF has numerous people, also in its "Legal team", which surely is at fault for this draft, and it would be quite nice if they could at least devote the same time to discussing here as we volunteers do. Yesterday I was asked whether I hadn't commented at #Purpose 2 (a section whose content I agree with) yet - quite simply, I have already said what is expressed there in a different section on this page or on the checkuser-l list or on IRC (where also WMF staffers were present / able to read it). To sum up, I see all the same concerns being had by multiple people and being mentioned again and again, yet WMF is more or less silent. So I don't really have any motivation to contribute to such a systematical analysis of the proposal, when I see no reaction to comments anyway. --MF-W 14:35, 21 October 2013 (UTC)

> I don't think it's entirely fair to treat the legal team as if they're ignoring us because they don't have immediate answers. Remember, these are people with (for the most part) regular 9-5 daily jobs, who are trying to tick the boxes that they feel need to be ticked before they can present any proposal to us. When Michelle says they are discussing our feedback, I tend to think they're doing just that - discussing our feedback and trying to figure out how to integrate it with whatever it is they feel the policy needs to accomplish, per whatever WMF reasoning underlays that need (which, yes, it would be nice if they could get around to explaining that part to us). I don't think there's any doubt that they now understand just how vehemently people oppose the proposal as it's written (and there's no reason people can't keep sharing their opinions on the current proposal while we wait for a response), but these are lawyers, who need to get their wording bulletproof before they send it out into the world. If we're not willing to wait for them to have a coherent response, the other option is a handful of legal team members chaotically attempting to share what they personally think might happen once a new proposal is offered, followed by them having to backtrack once things change a little, and an end result much like some of the less pleasant software deployments we've had lately where no one knows exactly what "the response" is and everyone's reacting to something different. Rather than going down that rabbit hole, let's give Michelle, Geoff, and team a reasonable chance to respond in detail (in business-day time, not constant-wiki time) before we start assuming that they have no intention of working with us. Fluffernutter (talk) 15:31, 21 October 2013 (UTC)

Fæ: Re: "not legally bound to respect a community consensus here," you seem to be a bit confused about how policies like this are enacted. The Wikimedia Foundation legal team can certainly propose rewrites and can advocate for changes to this policy, however the Board decides. wmf:Access to nonpublic data policy is the current policy and nothing that the legal team does can undermine this. Whether the Board itself is strictly bound to follow community consensus is a tricky question. :-) In this particular case, we seem to have the bold (rewrite) and plenty of discussion, but little editing, which is worrying and against the typical BRD process. If there are problematic parts of this rewrite, let's figure out what those are and address them on-wiki. I think certain pieces of this rewrite are completely uncontroversial. Those pieces, at least, should be simple enough to resolve/approve before we get to the more difficult and contentious pieces. --MZMcBride (talk) 16:26, 21 October 2013 (UTC)

> Thanks for your concern that I might be confused. However I believe that your assertions that the WMF board of trustees (a partially elected body) overrules a Wikimedia community consensus, and that this WMF legal document can be changed by using the practices used on the English Wikipedia for writing encyclopaedia articles are not terribly helpful. --Fæ (talk) 19:22, 21 October 2013 (UTC)

> > If it helps, BRD is also documented locally. :-) This isn't a legal document and it's strange that you would suggest that it is. This document is a proposed rewrite to a standing Board-approved policy. Regarding supremacy, the Board is indisputably the ultimate arbiter (cf. wmf:Bylaws).
> > I have considerable experience in meta-matters and I'm trying to help move the discussion forward. Unfortunately, I'm not sure the same can be currently said of you. --MZMcBride (talk) 20:17, 21 October 2013 (UTC)

> > > I'm obviously unwelcome and you seem determined to make this discussion unpleasant and personal, so I'll not bother contributing further. Good luck with it. --Fæ (talk) 20:42, 21 October 2013 (UTC)

Policy itself

Status: In discussion

We currently have wmf:Access to nonpublic data policy, passed by the Board in 2007. Does anyone think Wikimedia should *not* have this policy any longer (i.e., the Board should get rid of this policy)? I believe there's general consensus to continue having this policy in some form, but before we go any further, we should make sure. :-) --MZMcBride (talk) 02:47, 21 October 2013 (UTC)

- It seems reasonable to have a policy. --MZMcBride (talk) 02:47, 21 October 2013 (UTC)
- So it does. –SJ talk 20:33, 24 October 2013 (UTC)
- There should be a policy about it and access to nonpublic data needs to be restricted, imo. -**Barras talk** 09:35, 26 October 2013 (UTC)

Title

Status: In discussion

Assuming you agree with having a policy of this nature, we can start at the top. There's a discrepancy between this page's title ("Access to nonpublic information policy") and the policy from 2007 ("Access to nonpublic *data* policy"). Should the title be changed? Should this page be moved? Thoughts? --MZMcBride (talk) 02:47, 21 October 2013 (UTC)

- The titles should be synchronized. I don't really care which is chosen. --MZMcBride (talk) 02:54, 21 October 2013 (UTC)
- Synchrony improves harmony. –SJ talk 20:33, 24 October 2013 (UTC)
- If this policy draft is adopted by the Board, there will only be one title (Access to Nonpublic Information Policy) because it would be replacing the current policy, so it will be synchronized. The reason why I changed it to "information" rather than "data" was to be consistent with the privacy policy draft which refers to things like "personal information" rather than "personal data" and I thought consistency between the two policy drafts would be helpful in that regard. Mpaulson (WMF) (talk) 22:45, 30 October 2013 (UTC)

User-friendly summary

Status: In discussion

There's a "user-friendly summary" at the top of the page:

Text of user-friendly summary [show]

Is it necessary to include a summary with this document? Does anyone agree or disagree with including this summary? (Please focus only on the summary's inclusion itself, the content itself will be discussed below.)

- I'm not sure a summary is needed here. --MZMcBride (talk) 02:48, 21 October 2013 (UTC)
- I find it useful but perhaps it could be briefer; I worry at the first list for instance, as it may be interpreted as comprehensive. --SJ talk 20:33, 24 October 2013 (UTC)
- We have generally received a lot of positive feedback about the user-friendly summaries. While I personally like reading through entire policies, I completely understand that most people are not like me in that regard. We hope that the user-friendly summary will alert people to the most important parts of the policy and allow them to easily find and read the details of the sections that are the important to them. We try to alert readers to the fact that the summary is not comprehensive with the disclaimer on top stating "Disclaimer: This summary is not a part of the Access to Nonpublic Information Policy and is not a legal document. It is simply a handy reference for understanding the full Access to Nonpublic Information Policy. Think of it as the user-friendly interface." Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Purpose paragraph 1

Status: In discussion

Purpose paragraph 1 [show]

Does anyone agree or disagree with any part of this section?

- There's a semicolon splice ("content on the Sites;"). The final sentence doesn't make any sense. It says "Certain community members are entrusted with access to limited amounts of nonpublic information regarding others users, such as ...", but an example of limited nonpublic information isn't given. Instead, it tries to describe sockpuppeting to an outsider. This is a pretty strange sentence. --MZMcBride (talk) 02:51, 21 October 2013 (UTC)
- Thank you for pointing this out, MZ. As to your first concern, do you believe a comma would be more appropriate than a semicolon? As to your second concern, does this work better: To manage this immense task effectively, certain community members are entrusted with access to limited amounts of nonpublic information regarding other users. For example, a trusted community member who has "checkuser" rights could use those rights to investigate whether a single user is using multiple accounts in a manner inconsistent with Wikimedia policies. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Purpose paragraph 2

Status: In discussion

Purpose paragraph 2 [show]

Does anyone agree or disagree with any part of this section?

Scope paragraph 1

Status: In discussion

Scope paragraph 1 [show]

Does anyone agree or disagree with any part of this section?

- Does the "volunteer developer to access to nonpublic information" mean all Toolserver users? --MZMcBride (talk) 02:55, 21 October 2013 (UTC)
  - It's Labs now. --**Rschen7754** 18:53, 21 October 2013 (UTC)
    - Hi Rschen7754. Err, yes, I'm familiar with Wikimedia Labs. However, Toolserver users have access to the archive table and partial access to the user_properties and watchlist tables, among others. These database tables contain non-public information, which is why I asked the question I asked. --MZMcBride (talk) 20:19, 21 October 2013 (UTC)
- Does this include OTRS members? As we all know there is a major difference between stewards, checkusers & oversighters who have special access to the wikis and OTRS members who access correspondence that is separate from the wikis and where people know that their emails will be read by volunteers. I ask because it is worded *to view nonpublic information about other users*. OTRS members have access to nonpublic information but the term *users* usually refers to accounts on wikis which is possibly different from the clients send emails to the OTRS addresses. A significant part of the OTRS correspondence comes from people who never signed up as a user on any of our wikis. --AFBorchert (talk) 18:10, 22 October 2013 (UTC)

  This is worth specifying explicitly, as has been done in the past. –SJ talk 20:33, 24 October 2013 (UTC)
- MZ - This policy draft is intended to apply to Labs & Toolserver users who are granted access to nonpublic information. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)
- AFBorchert - This policy draft currently only includes OTRS administrators, but we really would appreciate input from the community in the discussion above about whether it should also apply to OTRS agents. I agree that there is some ambiguity due to the term "users". I think if OTRS agents were to be included, we would change that to something along the lines of "view nonpublic information about other users or nonpublic information submitted through OTRS". I am open to alternate wording suggestions though. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Scope paragraph 2

Status: In discussion

Scope paragraph 2	[show]

Does anyone agree or disagree with any part of this section?

- "Election committee" is too unspecific. Nobody knows which one. --MF-W 14:24, 21 October 2013 (UTC)
  - Hmm, I agree. And broadly, how is the determination made as to whether this policy is applicable to a specific group? --MZMcBride (talk) 01:25, 22 October 2013 (UTC)
- Hm... are OTRS administrators included but not other OTRS members? I would suggest not to enumerate some samples but try to give a precise definition (see above) and/or try to enumerate all groups to which this applies now (with possible more coming). --AFBorchert (talk) 18:13, 22 October 2013 (UTC)

  I agree with the value in a precise definition. That also helps clarify why this policy exists in the first place. However a list of all affected groups should not be too long, and makes a useful supplement. –SJ talk 20:33, 24 October 2013 (UTC)
- The groups listed there are only meant to serve as examples. The more specific scope is defined earlier by what the individuals can do -- "Community members with access to any tool that permits them to view nonpublic information about other users (such as the CheckUser tool);Community members with the ability to access content or user information which has been removed from administrator view (such as the Suppression tool); and Volunteer developers with access to nonpublic information." I would not be opposed to listing more examples of groups (or even all of the groups we can think of that currently fall into these categories, but I'm hesitant to make an exclusive list because new groups could form, those groups could change names, and sometimes there may be certain people within a group that need to identify (because they have access to nonpublic info) while other people in that group do not (because they only have access to public info). Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Requirements intro paragraph

Status: In discussion

Requirements paragraph 1	[show]

Does anyone agree or disagree with any part of this section?

- Please note that OTRS members and OTRS administrators are not chosen by the community of contributers. The question is if this point really needs to be elaborated here. I think it is best to remove this section. --AFBorchert (talk) 18:18, 22 October 2013 (UTC)
- I agree that "All... are typically chosen" may not be clear. The whole section could be reworded to focus on the requirements needed to get access to nonpublic data; rather than framing them as requirements for any particular selection process. –SJ talk 20:33, 24 October 2013 (UTC)
- That's a good point, AFBorchert. SJ - the reason why we included this section was to point out to more inexperienced users that the community members who have these access rights are trusted members of the community who have been vetted by the community. Do either of you have any suggestions as to how we could improve the wording in this section? Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

> How about this: *The following conditions are requirements that all community members should meet before being granted access to n.p.i.r. ("access rights"). These should also be considered requirements to be a candidate for any community-run selection process for a role that would convey such access rights.* –SJ talk 03:02, 3 November 2013 (UTC)
>
> > Hi SJ, I reworked the paragraph based on your suggestion. Thank you for your help! Mpaulson (WMF) (talk) 19:25, 9 December 2013 (UTC)

Requirements sub-point A

Status: In discussion

Requirements sub-point A [show]

Does anyone agree or disagree with any part of this section?

- This seems to unnecessarily disempower minors, considering how many of our extraordinarily competent, reliable, and talented administrators are smart high school students. If the concern is legal accountability, then a workaround involving a minor's legal guardian should be possible. If the concern is about practical accountability, then a signed statement may be equally effective (and most available remedies would be the same) for trusted community members who are not yet 18. Similar language was intentionally left as "may" instead of "must" in the previous version of the policy, and was not an oversight. –SJ talk 20:33, 24 October 2013 (UTC)
- I'm reposting my response from the discussion below just in case people missed it there: The switch from "may" to "must" was meant to get rid of the ambiguity. My understanding was, in practice, that all community members with access to nonpublic information (except OTRS agents) were required to be 18 years old and the age of majority for their jurisdiction. The reason for this in the current policy, as I understand, was to ensure personal accountability. From a legal standpoint, it is easier to hold an individual personally accountable if they are the age of majority. I saw no reason to leave the ambiguity of "may" in this draft policy if the purpose was to actually have an age minimum. That said, the age minimum (like anything in this policy draft) is not set in stone. It can be raised, lowered, or done away with all together. I'd like to hear what other community members think about the age minimum. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Requirements sub-point B

Status: In discussion

Requirements sub-point B [show]

Does anyone agree or disagree with any part of this section?

- This sounds as if the original document of identification has to be passed to the WMF. But this is probably not meant. I understand that the WMF needs some sort of proof of identification but I think it is best to move this to a separate point how this can be done. This section unnecessarily asks for identification documents (or possibly scans thereof) to be handed over to the WMF without considering alternative approaches. As pointed out above this is not just uncomfortable for many functionaries but also in conflict with local legislations. I would like to see here more openness towards solutions that provide the necessary proof of identification but which are more consistent with the preferences and the legal environments of the functionaries. It should be possible, for example, to handle this through the local chapters and possibly third parties. (For example, there exist identification services like Postident in Germany which could be utilized through the WMDE local chapter.) --AFBorchert (talk) 19:34, 22 October 2013 (UTC)
- I agree with AFB: I would strongly approve of any mechanism that does not require community members to send identifying documents to servers in a different country. –SJ talk 20:33, 24 October 2013 (UTC)
- Hi AFBorchert and SJ. This section was indeed meant to require a copy or scan of an identification document to be sent to WMF, not the original document. My apologies for the confusion. That said, we are very open to alternate forms of identification submission and retention and are soliciting suggestions from the community. You may want to see my response in the discussion below. I'd love to hear your ideas. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Requirements sub-point C

Status: In discussion

Requirements sub-point C [show]

Does anyone agree or disagree with any part of this section?

- This helps clarify what is being committed to. –SJ talk 20:42, 24 October 2013 (UTC)

Requirements sub-point D part I

Status: In discussion

Requirements sub-point D [show]

Does anyone agree or disagree with any part of this section?

- This requirement has a giant loophole. Why bothering about locked cabinets and password protection when arbitrary third parties with a non-disclosure agreement and unknown policies have unrestricted access to it? Leaks happen. And the best protection against leaks is to minimalize the amount of sensitive materials you collect. Hence, I do not understand why *physical copies of submitted materials* are required. A name and a postal address should be sufficient. (This is at least sufficient in Germany, see de:Ladungsfähige Anschrift.) --AFBorchert (talk) 19:47, 22 October 2013 (UTC)
- A few people have noted that (A) is not clear here. I do not understand the value of keeping other original documents around -- not trusting the initial authority used to verify them and needing to reverify? -- and would appreciate further explanation. There are valid reasons for people, particularly those who live outside of the US, to be wary of having personal documents permanently stored on servers in the US. The reasons for having access to originals that I can think of might be satisfied by either re-requesting them as needed or by having a document-escrow of the person's choice. –SJ talk 20:33, 24 October 2013 (UTC)
- Hi AFBorchert and SJ. As mentioned in the discussion below, we are very open to different forms of submission and retention and would like to hear your suggestions. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Requirements sub-point D part II

Status: In discussion

Requirements sub-point D part II [show]

Does anyone agree or disagree with any part of this section?

- In my opinion, this section should be killed. Retention (if any) should only happen during active use of the tools. A three-year period after seems unnecessary. --MZMcBride (talk) 03:07, 21 October 2013 (UTC)
- As pointed out above, it should be sufficient to keep the verified name and postal address of someone with access to nonpublic information. This would also be sufficient in the example you give. There is no need to keep copies of government-issued identifications. --AFBorchert (talk) 19:53, 22 October 2013 (UTC)
- This section seems too broad. An exception should be made for someone whose use of nonpublic information is being investigated (which may be the reason for loss of rights). But otherwise, there should be little need to retain most information. I can see keeping a very-limited historical record to avoid gaming the process: for instance, to keep a single person from identifying many times linked to different on-wiki identities. But some submitted materials (such as copies of formal IDs) could be deleted promptly; others (such as address/contact information) could be deleted soon after rights are given up. –SJ talk 20:33, 24 October 2013 (UTC)
- Thank you for your feedback on the retention period issue, MZ, AFBorchert, and SJ. I'd also like to point out that a related discussion is occurring above in case you want to see what others are saying. I'd also be curious about your thoughts on a 6 month following retirement of access rights retention period mentioned there. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)
- No opinion yet on the general idea, but I'd note that "If a community member ceases to have access rights, he or she should notify the Stewards" doesn't really make much sense. The Stewards are the ones who revoke access like this in the first place, so why would they need to be notified? — **PinkAmpers&** (*je vous invite à me parler*) 04:16, 15 November 2013 (UTC)
  - Hello @PinkAmpersand: as an update, that section has now been removed (https://meta.wikimedia.org/w/index.php?title=Access_to_nonpublic_information_policy&diff=6451564&oldid=6222708) from the policy now. Thanks, 22:32, 3 December 2013 (UTC)

Submitting new materials

Status: In discussion

Submitting new materials [show]

Does anyone agree or disagree with any part of this section?

- Again, this section implies that there is a need to keep copies of submitted materials. --AFBorchert (talk) 19:55, 22 October 2013 (UTC)
- Hi MZ! I wanted to repost what I just said in response to Risker in another portion of this discussion concerning the retention period in case people commenting here miss it up there.

> The reason why we had decided on 3 years is that when discussing potential periods for retention with the Ombudsman Commission, it seemed possible for an investigation concerning the actions of a community member with these kinds of access rights to still be ongoing 2 years after the community member in question had resigned their rights. This could be the case in a particularly complex investigation or one that did not come to the attention of WMF or the Ombudsman Commission until after the community member resigned their rights. That said, I understand that 3 years can be perceived as a long time and if the community believes that investigations of these kinds are all but rarely resolved in a shorter period of time than 3 years, I'm certainly open to hearing what they believe is a more reasonable length of time. Mpaulson (WMF) (talk) 21:40, 22 October 2013 (UTC)
>
> > Probably, if we look to European standards, a reasonable time is ≤\0. --Nemo 08:32, 28 October 2013 (UTC)

Submission methods

Status: In discussion

Submission methods [show]

Does anyone agree or disagree with any part of this section?

- Again, this is unnecessary as there exist alternative approaches to provide a proof of identity. --AFBorchert (talk) 19:58, 22 October 2013 (UTC)

Submission timeline

Status: In discussion

Submission timeline [show]

Does anyone agree or disagree with any part of this section?

- This paragraph fails to outline how the users with access rights will be notified and/or warned. And I think that some time should be given to develop alternative techniques to provide a proof of identity. (This does not need to be covered by this policy. There could be a process that approves alternative approaches.) --AFBorchert (talk) 20:05, 22 October 2013 (UTC)
- As I've mentioned above, we are open to alternative forms of proof of identity. However, I want to assure you that should any requirement submit identification documents or submit identifying information be adopted here, we will do whatever we can to notify any affected users about the new policy and what needs to be done. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Use and disclosure intro paragraph

Status: In discussion

Use and disclosure intro paragraph [show]

Does anyone agree or disagree with any part of this section?

- This section helps clarify what is at stake. –SJ talk 20:42, 24 October 2013 (UTC)

Use and disclosure sub-point A

Status: In discussion

Use and disclosure sub-point A [show]

Does anyone agree or disagree with any part of this section?

- This description does not match the activities of OTRS members. They are not always strictly in the business of preventing, stopping, and minimizing damage to the sites and its users. --AFBorchert (talk) 20:09, 22 October 2013 (UTC)
- Leeway for good judgement would be helpful here and in subpoint B. –SJ talk 20:33, 24 October 2013 (UTC)
- AFBorchert - As mentioned above, the decision as to whether OTRS agents should be included in this policy is still being discussed. However, I would be very interested in your suggestions as to how we could edit this section to include a description of what OTRS does. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)
- SJ - Could you clarify what you mean by providing leeway for good judgment? Do you have any suggested wording that would illustrate what you mean? Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

  A suggestion for AFB's point: *...solely for activities that protect and help the Sites and their users. Community members with access rights may only use those rights and the subsequent information they access under the policies that govern the tools they used...*
  I'm not sure of the right legal phrasing for good judgement. Perhaps "activities that, in their judgement, protect and help"? I'm not sure how important this is here. But it's usually not clear whether an action actually will have those effects; and the whole point of choosing people for their sensibility is that we are placing that trust in them. So it seems reasonable to me to call that out here. –SJ talk 06:08, 3 November 2013 (UTC)

    Hi SJ, I made some changes based on your suggestion, which hopefully addresses your point. Thank you for the suggestion! Mpaulson (WMF) (talk) 19:37, 9 December 2013 (UTC)

Use and disclosure sub-point B

Status: In discussion

Use and disclosure sub-point B [show]

Does anyone agree or disagree with any part of this section?

- In the current practice of CU cases, some nonpublic information possibly gets public like for example the information which accounts are related. When a CU case includes anonymous accounts identified by their IP addresses, this can be quite revealing. I do not see how this practice is covered by this section. Likewise, it is common practice to publish selected nonpublic information from OTRS correspondence. For example, in a permission case, OTRS members publish the before non-public fact that a copyright owner releases some media or text under a free license. What needs to be exercised is good judgement. Checkusers have a great responsibility when they publish their report of the CU results and likewise OTRS members must carefully judge what can be made public. This section as it stands does not address this. --AFBorchert (talk) 20:22, 22 October 2013 (UTC)
- See above. –SJ talk
- That is an excellent point, AFBorchert. Do you have any suggestions as to how to best address the OTRS scenario that will still protect against the public release of sensitive information often included in OTRS correspondence? As to the CU case, that example was brought up by someone else and

we are trying to figure out a way to address that situation directly in the policy. Any suggestions you have would be greatly appreciated! Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Hi AFBorchert. Just wanted to circle back on this and let you know that we added an additional disclosure scenario to this section in the new draft that hopefully addresses this issue. Thank you for your help! Mpaulson (WMF) (talk) 19:43, 9 December 2013 (UTC)

Penultimate paragraph

Status: In discussion

Penultimate paragraph [show]

Does anyone agree or disagree with any part of this section?

- This seems reasonable. --MZMcBride (talk) 03:10, 21 October 2013 (UTC)
- +1 –SJ talk 20:33, 24 October 2013 (UTC)

Final paragraph

Status: In discussion

Final paragraph [show]

Does anyone agree or disagree with any part of this section?

- There are two different e-mail addresses? legal@ and check-disclosure@? This seems confusing. --MZMcBride (talk) 03:09, 21 October 2013 (UTC)
- Actually there's a different situation which should be taken in consideration: if a checkuser living in, for example, Spain, is asked by local authorities to *quickly* disclose and IP of an user posting onwiki its intention to commit suicide. I know this kind of situation has been already managed, but WMF must take into account it re-writing a policy which seems to presume checkusers are criminals by nature. --Vituzzu (talk) 11:54, 21 October 2013 (UTC)
- MZ - legal@ is where anyone who wants to request user information from WMF should send those requests. If a community member receives such a request that falls out of the purview of their role or if they are simply uncomfortable responding to such a request, they should pass those requests onto WMF by sending it to legal@. In contrast, check-disclosure@ is where you should alert WMF that you have disclosed user information to a third party. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)
- Vituzzu - that scenario should be covered by "In the course of keeping the Sites and its users safe, community members with access rights must sometimes disclose nonpublic information to third parties. Disclosures of nonpublic information may be made to:...law enforcement in cases where there is an immediate and credible threat to life or limb;" Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Notifications

The following discussion is closed: ***closing this since it's been more then a month without response. I think we've reached out to all groups that need it (some a couple times) but if there are others who need it please let me know, I'm happy to try and reach out to others. Will archive in a couple days unless reopened. Jalexander--WMF 20:35, 9 December 2013 (UTC)***

As I already asked on wikimedia-l without answer from WMF: were all the checkusers, OTRS volunteers etc. specifically notified about this draft and discussion which matters them directly, on their email addresses or talk pages? It would be better if the WMF did so, as only WMF knows why we're having this discussion, but time is running: if they don't plan to, can someone use global message delivery to notify them? Objections? --Nemo 06:52, 24 October 2013 (UTC)

I know all CU/OS/stewards received an email, but I get the feeling that some groups got left out, especially as there is no concrete definition of who is affected by this. --**Rschen7754** 07:00, 24 October 2013 (UTC)
(e/c)All checkusers, oversighters and stewards were notified by email. I mentioned this above somewhere as well after being asked about it. I know that the enWP ACC tool users (who identify because of their IP access on the tool) were also notified. I have not notified OTRS agents yet because we had not determined exactly how they would be affected, the policy as written did not envision including them (similar to the current policy which puts them into a special category) and the privacy policy was written with that assumption as well (lack of privacy when you email) though I know that it has come up and we would probably need to put an exception into this one similar to the current one. That wasn't added when it was brought up earlier because of the ongoing discussions, my guess at the moment (assuming we continue to check IDs) is that we will have a separate discussion to figure out OTRS which they will obviously have to be notified about. When it came to that I'd probably work with the OTRS admins because I know they have sent mass emails to all agents before. Jalexander--WMF 07:07, 24 October 2013 (UTC)

Actually I think that all users should be informed about this major change, no matter what user groups they belong to. Of course it is more important for the users who are directly affected by this, but there might be people out there who plan on becoming OTRS agents, checkusers or oversighters on their projects and don't know that this policy may be changed in future. There might be people who want to run for the next steward elections, not knowing about this. Not only users with access to nonpublic information should be informed, but also the people whose nonpublic information we are talking about. I'd like to see some notification about this for all users rather soon. It's not fair to inform only a subset of people instead of all! -**Barras talk** 08:10, 24 October 2013 (UTC)

OTRS users sure weren't - David Gerard (talk) 13:46, 24 October 2013 (UTC)

As Rschen7754 notes, some possibly affected user groups were likely not notified because there's ongoing ambiguity about what the scope of this proposed rewrite is. I believe the current interpretation is that this proposed rewrite would only apply to OTRS administrators, not OTRS users. But at this rate, I think the entire rewrite will be scrapped. --MZMcBride (talk) 14:20, 24 October 2013 (UTC)

@Risker: Would functionaries-en subscribers be required to identify, even though many of them are ex-arbs who no longer hold CU/OS? --**Rschen7754** 18:55, 24 October 2013 (UTC)

If it's about notifications I know I emailed them when we sent out the CU/OS notifications (to make sure they got it). Whether they would need to re identify even if they no longer hold CU/OS to remain on the list is an interesting question I'm not sure had been thought about... Jalexander--WMF 00:09, 25 October 2013 (UTC)

It applies to me and just a couple others (although I guess I might also have to identify for OTRS). It's not like a bunch of folks at the WMF don't already know who I am, so I don't have any problem with identifying again in principle, but it would be a pain... **NW** (*Talk*) 22:29, 25 October 2013 (UTC)

yeah, as usual on these types of edge cases it would have to be a bit of a case by case analysis (since circumstances change etc) but talking with Philippe a superficial look at functionaries-en says that we would likely not force non CU/OS users on the list to identify. Jalexander--WMF 22:41, 25 October 2013 (UTC)

- Note: I'm reaching out to the OTRS admins now to alert all OTRS users of this discussion and the discussion above about if we should include them in the policy. Jalexander--WMF 21:42, 25 October 2013 (UTC)
- Why are not **all** users informed about this discussion? It's good that the people with access to nonpublic information are informed, but I fail to see a reason why the people whose information we are talking about are not informed. I think that everyone should have their say here, and I think everyone deserves it to be informed. Of course the CUs, stewards etc etc are more affected by this, but trying to look at this from outside, as a normal user, I'd like to be informed about that change. There might be users who want to know who deals with their private/nonpublic information and what the rules about this are like. Even thought that is an open discussion and everyone may find this place themselves, I doubt that all users are actively searching for such stuff. Looking at the page, mostly/only people who were informed take part in that discussion. Other people may also have good ideas and wish to comment. I'm really disappointed about the information flow about this. -**Barras talk** 12:53, 26 October 2013 (UTC)

The idea was that we were doing this as part of the privacy policy discussion because they are very tightly linked (and changes in here may require changes in the privacy policy). We had a blog post and mailing list announcement (both of which had a whole paragraph talking about this policy) and ran banners both to logged in and anonymous for the privacy policy with links to the blog post in the introduction and links to this policy and discussion on that feedback page. Given that the privacy policy was the center piece of the discussion and we were talking about this in that context it did not seem to make sense to have separate banners for this policy (especially since we were sharing with Wiki Loves Monuments and Fundraising, both of which were pushing for us to lose less space already.. which we were telling them no on). If people think that we should do some more out reach I'm certainly open to it, this is also why we had such a long (and somewhat open ended) feedback period to make sure we could try and get as wide a net of feedback as well. I've always somewhat intended to throw the banners on for another week at one or two different periods over the course of the 4-5 months we are discussing. Jalexander--WMF 10:32, 27 October 2013 (UTC)

Agreed, I work in Account Creation, and I see personal info with every request. Anyone who works with personal information should be notified of this discussion. --Sue Rangell (talk) 19:52, 2 November 2013 (UTC)

feedback from otrs agent

The following discussion is closed: ***Closing given how long it has been since the last edits and the large changes on the draft since then. Will archive in a couple days unless reopened. Jalexander--WMF 20:51, 9 December 2013 (UTC)***

As for I, I have totally given up with the idea of preservation of confidential data when the US are somehow involved (if the NSA is already involved in recording German president phone conversations or French diplomatic department communications, who are we to hope that our every steps can be private anyway ?).

My trust in WMF ability to provide security to our private information also dramatically dropped with the password leak a couple of months ago.

Hi Anthere. I completely understand your concerns here. The actions of the NSA have shocked and upset us all. As for the hashed password leak, that was a very unfortunate incident and one we are working to ensure never happens again. Mpaulson (WMF) (talk) 21:40, 30 October 2013 (UTC)

So what are the risks left ? I see mostly three main ones

disagree with preservation of digital version of id papers

1) that a digital version of my passport get in the hands of scammers. We know some of the risks associated to this, one of which being identity theft. Collection of a bunch of private data (name, email, phone number, postal address...) is one thing. Preservation of official identity paper is another.
I think that's a non-acceptable risk.

> We are open to ideas about how the identification documents are stored. Are you against any kind of digital submission or retention of documents or are there certain security measures like encryption that would make this option more palatable to you? If you do not think any digital submission or retention is safe enough, would mailing you identification documents and retaining them in a safe be a sufficient alternative? You may want to look at a related discussion below regarding whether storing identifying information rather than copies of the identification documents themselves would be sufficient and leave some thoughts there as well. Mpaulson (WMF) (talk) 21:40, 30 October 2013 (UTC)
>
> > Answered below. Anthere (talk)

disagree with disclosure of agent private information to community members not bound to the non public information policy

2) that WMF disclose private information about us (OTRS member for example) volunteers to other volunteers, who may not even be identified in the least (as in "arbitration committee members").
Main risk associated imho would go from mild online bullying to severe irl mishandling. I have very acute memory of this sick person sending me emails threatening my life and the life of my own kids when I was Chair of WMF. I was happy he was in the USA and me in France. I was not happy he knew of my postal address. And I was scared when I met him at the WMF doors irl.
Disclosing private information about us to a lawyer or a policeman is one thing. Disclosing private information about us to an "unknown" wikimedia member not bound by similar rules related to private data is unacceptable.

> I'm a little confused about this comment. WMF would not disclose information from the submitted identification documents to other volunteers. Under the applicable clause in this draft, "The Wikimedia Foundation will not share submitted materials with third parties, unless such disclosure is (A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department; (B) required by law; (C) needed to protect against immediate threat to life or limb; or (D) needed to protect the rights, property, or safety of the Wikimedia Foundation, its employees, or contractors." I assume you are referring to the text in the subsection following stating: "Sometimes, the Wikimedia Foundation or a user community committee will need to contact a community member who formerly had access rights about his or her usage of those rights. For example, the Arbitration Committee may need to complete an ongoing case they are examining or the Wikimedia Foundation may need to notify you of receipt of a legal document involving that community member." This section was meant to explain the reasons for retention of your identification information. WMF would not give your identification information to other volunteers in this situation. We would contact you using the information you submitted to us to let you know that ArbCom needs to get ahold of you regarding an ongoing case. Would clarifying that in the policy draft help? (And obviously let me know if I'm misunderstanding your concern here and therefore inadequately addressing it.) Mpaulson (WMF) (talk) 21:40, 30 October 2013 (UTC)
> Yes, if this is what you have in mind, I think a clarification of the text would be best. I read that our data may be given to arbcom members for example. Anthere (talk)

ask for mandatorily notification of non public information disclosure about agent from WMF to concerned agent

3) last, that WMF disclose private information about us without having the obligation to inform us it did so.
The draft proposes that *The Wikimedia Foundation will not share submitted materials with third parties, unless such disclosure is (A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department; (B) required by law; (C) needed to protect against immediate threat to life or limb; or (D) needed to protect the rights, property, or safety of the Wikimedia Foundation, its employees, or contractors.*
This is vague enough that it may happen that our private data is disclosed to about whoever (who will access our private data thanks to this "permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department" ???), possibly without us knowing.
Consequences may be various (being citing in a legal case without even knowing; having personal information disclosed to spammers or scammers; being sued by an "unhappy customer" after we failed to fix his case on otrs etc.)
A good part of benefit of this agreement would be that covered person better feel accountable.
I think a fitting balance would be that WMF agree to mandatorily inform ANY covered person WHEN and to WHOM his/her information has been disclosed. Accountability both way. Naturally, WMF would also engage itself to inform us when it fucked up (as it did well with the password leak) Anthere (talk)

> I agree completely. In fact, the protections that you speak of are currently in the forthcoming "Requests for User Information Procedures and Guidelines". We are working with the EFF to finalize it and will be releasing it publicly soon. The very purpose of these guidelines is to let anyone -- litigants, governments, police authorities -- who wants user information from us know what standards they need to meet before we are willing to release any user information. The guidelines also specify that our default position is to inform the affected user (if we have contact information for them) that such a request has been made and by whom so that the user can use any legal remedies available to them to stop the release of their information. Mpaulson (WMF) (talk) 21:40, 30 October 2013 (UTC)
>
> > Good (great); Waiting for the forthcoming RUIPG then. Anthere (talk)

Comments

Good points and some scary but true illustrations. I would like to add that I would be a lot more comfortable if I knew that were a scan of my passport to ever be leaked on the internet and I was then subject to identity theft, was then forever internationally blacklisted for credit, falsely thought to be a terrorist by the NSA and could never do business in the USA, or suffered other damages, that the WMF (or their agent with authority to hold the records) had excellent data protection insurance that I could then easily claim something in the order of $2,000,000 compensation to make me feel better about my damage and distress caused by my unpaid volunteer work that happened to require identification. Thanks --Fæ (talk) 14:16, 26 October 2013 (UTC)

Agreed. Anthere (talk)

WMF has secured insurance coverage as deemed appropriate by our Finance department.Mpaulson (WMF) (talk)

Sounds good, as the volunteers that are protected by this insurance, can we look at it please? I would like to know how much I am covered for if someone emailing OTRS tries to take me to court for whatever reason and requires the WMF to reveal my legal identity. Thanks --Fæ (talk) 22:46, 30 October 2013 (UTC)

After Geoff's clarification in a previous section, I now know that there is no "data protection insurance" for volunteers, nor does the WMF have any plans to fix this lack of insurance cover. In this context I feel the answer given that "WMF has secured insurance coverage as deemed appropriate" when the fact is there is no such insurance, was more political spin than a real answer and considering the intention of my comment was extremely clear and illustrated with examples, I feel this was misleading. In practice this means that to get any damages/compensation after suffering identity theft or fraud, a volunteer would probably have to sue the WMF for mishandling their personal data so that in turn the WMF could claim this against insurance that protects them but not the volunteers. I hope that answers to other questions on this page by the WMF have been more straight-forward. --Fæ (talk) 10:43, 15 November 2013 (UTC)

- Thank you for posting these comments here Anthere, I was about to copy them from the mailing list and noticed you already had. Would you mind if I (or you) either adjusted the header or split off #3? I want to make sure that the specific comment on notification gets attention (the other pieces are important as well but I think they are generally covered under other sections which I know are already on the list for discussion and consideration). Jalexander--WMF 06:12, 27 October 2013 (UTC)
  - is that okay this way ? If not clear enough, do not hesitate to edit my part. Anthere (talk)

Illegal

The following discussion is closed: ***Closing given how long it has been since the last edits and the large changes (including removal of physical ID) on the draft since then. Will archive in a couple days unless reopened. Jalexander--WMF 20:52, 9 December 2013 (UTC)***

In the Netherlands it is illegal to request a copy or scan of a passport or ID card. In the private sector only banks and employers are an exception in that by law.[1] (http://www.telegraaf.nl/binnenland/20791004/__Kopietje_paspoort_verboden__.html)[2] (http://www.cbpweb.nl/downloads_rs/rs_kopie-identiteitsbewijs.pdf) In all other cases it is forbidden to make copies or scans of it. By law we must report any organisation that still requests it, as it is illegal. Romaine (talk) 21:22, 26 October 2013 (UTC)

On the tangential subject of national variations—a slight wrinkle for UK citizens is that we are not required by the state to have any standard ID, and there is no standard identity card even if I wanted one. My passport happens to be the only photo ID I possess, so when that expires next month, I will not have any form of official photo ID to present to anyone. As it happens I have an old form of driving licence, no photo, again UK government does not require me to update to the photo-ID driving licence which was introduced in 1998, so it is just a big piece of paper; it confuses the hell out of people when I try and hire a car. --Fæ (talk) 21:51, 26 October 2013 (UTC)
Hi Romaine, can you clarify the relevancy of the point you make above? Since the WMF is not located in the Netherlands, it's unclear to me. **Nathan** T 14:28, 27 October 2013 (UTC)

Aren't WMF's esams and knams servers near Amsterdam, The Netherlands? --**Krenair** (talk • contribs) 14:38, 27 October 2013 (UTC)

Nathan, the actions of the WMF in enforcing policies for Wikimedia volunteers should not just be literally "legal", but being seen as a global charity ought to be lawful. In this case though the WMF may argue the case that it would not be *technically* breaking the law in the Netherlands, the common sense rules for NL businesses and the public still apply. I suggest taking a look at the documents that Romaine has linked to, they seems to support the exact same concerns that have been raised by other volunteers on this talk page. --Fæ (talk) 16:59, 27 October 2013 (UTC)

Romaine, is it also illegal to *provide* such copies? --Nemo 20:13, 27 October 2013 (UTC)

Romaine, how does a business that needs to identify you in the normal course usually do it in NL then? (For instance, if you rent some expensive bit of equipment, the lender would normally need to have some way to keep you accountable).
— Coren (talk) / (en-wiki) 14:04, 28 October 2013 (UTC)

> They probably look at the ID card and simply note down the needed data (address, name, date of birth) or put it into their data bank without keeping a scan/copy of the ID card. We've similar laws in Germany. The ID card my be used to verify the data/person, but it is not allowed to retain copies of it. See German laws §§14-20 PAuswG. -**Barras talk** 16:06, 28 October 2013 (UTC)
>
> > Just as Barras says, showing the ID card is sufficient (in most cases noting down the info from the card isn't needed). Scanning/copying is only allowed in case of a juridical base: a legal obligation. In other cases it is forbidden to copy/scan. The Dutch government is keen on preventing identity fraud and other forms of fraud with identification. Romaine (talk) 01:35, 29 October 2013 (UTC)
> >
> > > If this is confirmed, it's obvious the policy will have to include at the very least an exception for the Netherlands (and any other country forbidding to make copies of identity documents): the WMF can't solicit, let alone force, anyone to commit illegal activities. --Nemo 06:52, 29 October 2013 (UTC)
> > >
> > > > Can they do it with people in other countries though? I would've thought that since they have servers in the Netherlands, Dutch law applies to them. --**Krenair** (talk • contribs) 16:12, 29 October 2013 (UTC)
> > > >
> > > > > IMO it would better to establish a standard that works for everyone, rather than have some people with copies of IDs and others with just stored information. Ajraddatz (Talk) 02:07, 30 October 2013 (UTC)

Hi All! Thank you for sharing your concerns here. We are certainly open to ideas on how identification should be handled. Accordingly, I'd like to get some thoughts on a few things below (and please feel respond in-line for the sake of clarity.) Mpaulson (WMF) (talk) 19:02, 30 October 2013 (UTC)

> First, does anyone have alternate links to the information Romaine provided? I seem to only get error messages when I try them. Mpaulson (WMF) (talk) 19:02, 30 October 2013 (UTC)
>
> 1. rs_kopie-identiteitsbewijs.pdf on web.archive (http://web.archive.org/web/*/www.cbpweb.nl/downloads_rs/rs_kopie-identiteitsbewijs.pdf)
> 2. Telegraaf article on web.archive (http://web.archive.org/web/20131101064727/http://www.telegraaf.nl/binnenland/20791004/__Kopietje_paspoort_verboden__.html)
>
> --Fæ (talk) 06:53, 1 November 2013 (UTC)

> Second, given the restrictions on providing copies of identification documents to third parties in some countries and the lack of requirements to have any identification documents in other countries, what do you all think would be an acceptable method of checking identification? Would simply submitting your real name and current email address suffice? Should a mailing address or telephone number be required? Are there alternate ways that one can prove their identity other than submission of a government-issued identification document? Should everyone be required to submit their information the same way or should there be different options for people to choose from? If the latter, how do we ensure that the different options are of roughly equivalent credibility? Mpaulson (WMF) (talk) 19:02, 30 October 2013 (UTC)

> Third, should the information submitted (whether it be a copy of an identification document or simple submission of a name and email address) be verified in some fashion? If so, how? If not, why not? And if so, should it be periodically re-verified and how often? Mpaulson (WMF) (talk) 19:02, 30 October 2013 (UTC)
>
> > Firstly, a simple method to verify a postal address is to send a letter to it with some token that allows to confirm that it was successfully delivered and received by the intended recipient. This approach is simple and does not break any laws. It just takes some time.
> > Secondly, I do not see a problem if multiple options are provided where people can freely chose from. You do not need an equivalent amount of credibility, just some minimal threshold which is to be met. No method of identification is safe against falsification. But please remember that you are requiring identification from people who have already trust from the community.
> > Thirdly, it should be sufficient to simply ask all volunteers who work under this policy to update their address etc. if it changes. --AFBorchert (talk) 19:35, 30 October 2013 (UTC)
> >
> > > And obvious cases should please be handled as obvious cases. Some prefer pseudonyms but many of us work already with their real name all the time (like me). You will find my full name on all my major wiki user pages, you find a backlink to Wikimedia Commons at my private website (http://www.andreas-borchert.de/), whose domain is owned by me (there are public records with my name and address at DENIC), and whose IP address (currently 217.10.8.60) when submitted to RIPE delivers multiple contact records including AFB13-RIPE (https://apps.db.ripe.net/search/query.html?searchtext=AFB13-RIPE&searchSubmit=search) which delivers my full address including phone number. You need of course a general solution for the identification problem. But I would appreciate it if obvious cases (like mine) need no further bureaucratic procedures. --AFBorchert (talk) 19:49, 30 October 2013 (UTC)
> > >
> > > > Thank you for your thoughts and suggestions, AFBorchert.
> > > >
> > > > > Postcards to verify address have been mentioned multiple times. Another option, to verify at least name and potentially more, is a symbolic payment: PayPal uses it, it's the only legal identification method for bank accounts "portability" in Italy, etc. A 0,01 € bank transfer to your SEPA bank account will be an extremely easy and cheap option for many in EU (you could also pay it back, I hope WMF doesn't pay fees for such SEPA payments). It wouldn't work for everyone, of course; just adding to the list of ideas. --Nemo 20:09, 31 October 2013 (UTC)

> I would like to add into the mix that any trusted user that is, or has been in the past, a trustee or director of a legally incorporated Wikimedia Chapter or Thematic Organization has public records of their directorship available as a public record. I believe that in most countries this means that there is a record of their directorship that is fairly easy to link to on the internet. Directorships have been verified against legal IDs (which acts as protection against money laundering) and have been accepted by the WMF under the Chapters Agreement. Personally, I don't mind sending the WMF a link to my online directorship records as they are already a public record; this avoids the bizarre discussion we will have when the WMF asks me for valid photo ID and I say I don't have any, as it is not required in the UK. --Fæ (talk) 07:04, 1 November 2013 (UTC)
>
> > I work in Account creation, and I see personal info in almost every request. As an identified editor, I had no problem with the scanned ID, and will happily do it again. A symbolic paypal payment is also acceptable. I don't think a postcard would work for me. I live in a remote area and sometimes I get mail 2-3 months late. (although I have no problem with that as long as that is taken into account) I am worried a bit that there will soon be an admin requirement for this. I don't want to be an admin, but more and more I am finding that it is necessary to become an admin just so that I can do the things I do on Wikipedia. --Sue Rangell (talk) 19:42, 2 November 2013 (UTC)

I agree with most comments made there

- most businesses requiring ID information record first name, last name, dob, country-region-date for issuing the ID document, and unique number of the document. They do not keep a copy of the ID but usually ask to "see" the ID paper and record data themselves in front of you. Ideally, it would be a declaration of honour you would require from us. Alternatively, we sent (in some encrypted fashion if possible) the scan, you record the data and you delete the scan.
- I recently moved; wrote my US bank to record the new postal address; they wrote to my former address for confirmation and ask me to send back a document. Very simple way to check addresses. Easy to do the same with the email address for confirmation. May be renewed once a year if suitable (as in… once a year, WMF send a new year eve wish card to all its agents and agents have to answer "thank you" :))
- Token payment is an option as well
- and yes, please rely on cases where people are or have been board members or staff within chapters (or on WMF board for that matter ;)). All those people already disclosed mandatorily their ID data to their chapters.
- use opportunities of face to face meetings to do an irl ID check-up (wikimania, wikimedia events when WMF staff is there) rather than electronic one.

Anthere (talk) 10:24, 7 November 2013 (UTC)

Statement from user:aschmidt

The following discussion is closed: ***Closing given how long it has been since the last edits and the large changes on the draft since then. Will archive in a couple days unless reopened. Jalexander--WMF 20:52, 9 December 2013 (UTC)***

One of the most fundamental priciples in data-protection law is that no data shall be collected and saved unless it is absolutely necessary to do so. There is no point in collecting scans of OTRS sysops' and maybe even agents' official documents. If the WMF is interested in learning who works in OTRS it would suffice to store their names and adresses only. This is why it would be disproportionate to keep any scans. For the same reason there is no legal justification for keeping all this data for years after a Wikipedian has ceased to contribute to OTRS.

To put it clearly: The Wikimedia Foundation is a big U.S. foundation worth millions of Dollars that runs hundreds of huge websites in some 200 languages. Those volunteering in the OTRS team provide online support for free that the Foundation would otherwise have to pay for by hiring agents. When I contribute for free as a volunteer to OTRS I expect the WMF to except us from any liability whatsoever as long as we are acting in good faith. Also, I think it is not only a matter of whether only OTRS sysops or agents, too, should be subject to this new policy. If it would be enacted I would quit German-language OTRS even as an ordinary agent.--Aschmidt (talk) 19:30, 28 October 2013 (UTC)

> Hi Aschmidt! Thank you for your sharing your feedback. I'd like to hear more about what concerned you about this draft. We are trying to change this draft such that it gets to a point that most people are comfortable with its requirements. We certainly are not trying to drive you away from being an OTRS agent!
>
> First, do you believe that WMF should keep any kind of identification policy at all, as discussed above? If we do continue to have an identification policy, you mentioned that you think real names and addresses would suffice. Did you mean email address or physical addresses? What way would you feel comfortable submitting that information? Do you think that information should be verified in a particular way?
>
> You have also indicated that you believe retention of such information for 3 years following the retirement of access rights is too long. What would be a more appropriate retention period in your eyes? There has been a more detailed discussion about this particular topic above that might interest you.
>
> And finally, if we do retain an identification policy of some kind, do you believe that OTRS agents should be subject to it (assuming that the policy adequately addresses your other concerns)? Why or why not?
>
> Thanks again for taking the time to help us make this policy draft better. Mpaulson (WMF) (talk) 18:35, 30 October 2013 (UTC)

Stuff to think about

The following discussion is closed: ***Closing given how long it has been since the last edits and the large changes on the draft since then. Will archive in a couple days unless reopened. Jalexander--WMF 20:53, 9 December 2013 (UTC)***

Just to make clear, I do not wish to reidentify if this policy becomes live. I identified when people could still go to a local WMF office and then make themselves clear for a local WM office member, and so identify themselves. I send my ID two years ago and then it was destroyed and only a few basic stuff were needed (name, date of birth, nationality etc). I cannot believe that rewriting an exisiting policy which works fine for over six years is more important than improving existing tools and developing new tools for the hardworking community. You even make it harder for the volunteers to do their work. Also I'm not comfortable with the WMF keeping my ID somewhere in the USA, or even with some basic information. You know who I am. That should be enough. You should spend time at the tools we actually need (finalizing SUL, global rename, global checkuser, global blocking etc) instead of writing new fancy tools such as wikilove, the thank button and visual editor. I know it's important to attract new volunteers, but please do your best to keep the existing ones as well. FYI, I'm one of the most active stewards and meta CUs and the active CU on commons. It's your loss if I quit, not mine. I have enough useful things to do. And I know more people think about this the same as I do. Some might say: "well, those are the consequences if you change a policy. Approximately 10% quits." But I disagree with that. You should listen to the people who do the work. And do something with their feedback. I'm also waiting for three months almost for an answer of Philippe (unrelated to this). That illustrates how the staff works here with the volunteers I guess. It's easy to answer easy questions, but less easy to answer to more difficult questions apparantly. Thanks for your time. (And don't get me wrong, I am happy with some things, though not with everything...) Regards, Trijnstel$_{talk}$ 12:24, 3 November 2013 (UTC)

> Hi Trijnstel - Thanks for your comments, which definitely resonate with me. We actually take the feedback from volunteers in these consultations quite seriously - and modify or propose ideas accordingly. I agree that, if we require improved identification, we probably should explore avoiding a new identification with the same information. In response to the feedback, one proposal - which we make above - is to eliminate all identification requirements, and that would address some of your concerns, I believe, and in fact render the job of volunteers a bit less administrative. I'm sorry about the lack of response for one inquiry. If you resend your question to me, I will try to get someone to handle it for you. I completely agree that your quitting is our lose ... so please don't. :) Our volunteers are so critical to the movement and its mission. Without any exaggeration, you are the inspiration for all of us. Geoffbrigham (talk) 00:41, 6 November 2013 (UTC)
>
> > Hi Geoff. Thanks for answering. Here a follow-up as I don't really get what you mean. You say:
> >
> > - *"if we require improved identification, we probably should explore avoiding a new identification with the same information"* - so that would mean that the re-identification rule would still apply in the new policy (with the 3 year retention in it), but what do you mean with "new identification with the same information"? Saving name, age etc? (which I'm not fond of either)
> > - *"one proposal - which we make above - is to eliminate all identification requirements"* - so everyone can identify then? Even if you're not yet 18 or 21 (depends in which country you live)? That's a really bad idea imho. And it doesn't address my concerns at all, which is that the Wikimedia Foundation will keep the ID of the volunteers who just want to help. With the posibility to sue them if they do something wrong, instead of making the WMF responsible. Or maybe I didn't understand you correctly?
> >
> > > Sorry, I was not that clear after thinking about your question some more. I agree with you in principle that we need to minimize the burden of identification and reidentification on our volunteers. So I'm open to an easier re-identification procedure where we retain the basic information (name, date of birth, point of contact). With known volunteers, we could figure out simple ways to get that information to hopefully decrease the administrative burden. I do think that, if we require identification, we would need to record the name, date of birth, and contact information to be consistent with the intent of the applicable Board resolution. We do not need to keep the identification, but we do need to record the identifying information to be honest by the Board resolution.
> > > If we eliminated the identification process at WMF, we would simply rely on the community processes to properly vet volunteers per the age requirements and capabilities; that way WMF would be retaining no personal information on our volunteers. (After reading the full consultation, that is an approach I'm beginning to consider seriously, though we would need the WMF Board to agree.)
> > > As to responsibility of the users, we could put limits on the liability, which I discuss a bit more here. To be clear, it is a hard case to imagine where we would ever sue a legitimate volunteer who is acting in good faith. My concern is about someone who, in bad faith, for example sells nonpublic information for personal gain. That is the "test" case that I'm trying to figure out. As I say, I discuss this a little more here. Thanks for the great questions and expressing your legitimate concerns, which I take quite seriously. Geoffbrigham (talk) 23:47, 6 November 2013 (UTC)
> > >
> > > > But then would local communities be responsible for handling private information? On English Wikipedia, ArbCom does vet volunteers, but I would feel uncomfortable with them having my personal info. On Commons/Wikidata/Meta etc. it's just a vote by the community. --**Rschen7754** 09:07, 7 November 2013 (UTC)
> > > >
> > > > > Under the proposed approach, I think it would be up to each community to decide what the acceptable standard would be and whether identification would be required. The number of questions that have arisen with respect to WMF holding the information and frankly the arguable ease by which one might be able to submit a fraudulent ID suggest to me that we should seriously consider eliminating all WMF identification. We would need to be clear in the privacy policy that WMF cannot identify those who have access to nonpublic information but

that communities are free to set their own standards, including identification processes. We could set minimum standards, such as requiring those with access to keep the information confidential (even if they are not identified). It is not a robust approach, but, if I am reading the discussion fairly, most in this community consultation seem to be rejecting a strong verification, accountability system that is manageable in a practical way, which is fine as long as we are honest about it in the privacy policy. Geoffbrigham (talk) 19:45, 22 November 2013 (UTC)

Btw, no need to look at my question, Maggie said a few days ago that she would take care of it. Trijnstel$_{talk}$ 16:33, 6 November 2013 (UTC)

Thanks, let me know if you need anything there. Geoffbrigham (talk) 23:47, 6 November 2013 (UTC)

WMF board, FDC, etc.

The following discussion is closed: ***Closing given how long it has been since the last edits will archive in a couple days unless reopened Jalexander--WMF 20:54, 9 December 2013 (UTC)***

I assume that candidates for the WMF board, FDC, etc. would have to identify regardless of what is decided here - is that correct? --**Rschen7754** 09:28, 6 November 2013 (UTC)

Correct. Geoffbrigham (talk) 20:06, 22 November 2013 (UTC)

That would be my understanding under the inescapable international requirement to meet money laundering regulations. Both trustees on the WMF board (once elected) and FDC members have influence over the disposition and management of significant funds. I would support some form of independent but legally meaningful identification (it does not have to be through the WMF) for anyone in any Wikimedia organization taking a direct part in how significant funds are spent. Saying this, I think there is room for less onerous requirements for "insignificant" funds, such as being on a judging panel for prizes but not in control of the budget allocated, where the total being given away is less than $1,000. In those circumstances the fact that Wikimedia *should* always default to open processes, means that if someone starts giving their mates prizes in an arbitrary way, or the competition was not properly promoted so only someone's pals even take part, then at some point there will be public complaints; knowing this, anyone that fiddles the system for small amounts of money would be pretty daft and find themselves having to pay the money back. I have put "should" in italics here as I have recently found myself arguing the case for openness within Wikimedia organizations in situations I never expected and sadly find myself becoming more jaded over time with the ability of our community to implement this theoretical ideal. --Fæ (talk) 16:41, 6 November 2013 (UTC)

Pedantic lawyerly point about use of "age of majority"

The following discussion is closed: ***Closing given how long it has been since the last edits and large changes in draft since then. Will archive in a couple days unless reopened Jalexander--WMF 20:55, 9 December 2013 (UTC)***

The current policy refers to the user being "over the age at which they are capable to act without the consent of their parent in the jurisdiction in which they reside." The proposed policy instead refers to the user being "at least the age of legal majority under the laws of the jurisdiction in which they reside." I would suggest that the existing wording (or other similar wording) is preferable because it corresponds more precisely with the expressed purpose of the age requirement, viz. ensuring that users with access to sensitive information have "legal accountability" for their actions. Let me illustrate by reference to New Zealand law. The age of majority in New Zealand is technically 20 (Age of Majority Act 1970, s 4(1)).[3] (http://www.legislation.govt.nz/act/public/1970/0137/latest/DLM396495.html) However, 18 and 19 year-olds are fully legally accountable for their actions and their parents have no legal authority over them. Contracts can be enforced against them (see the definition of "minor" in the Minors' Contracts Act 1969, s 2(1)).[4] (http://www.legislation.govt.nz/act/public/1969/0041/latest/DLM392356.html) So the proposed policy would seem to exclude 18 and 19 year-olds in New Zealand, despite this being completely unnecessary in terms of the rationale.

Interesting point. If someone is 18 or 19 in New Zealand, can they enter into a binding contract by themselves without a parental cosignatory? Geoffbrigham (talk) 22:08, 15 November 2013 (UTC)

Yes, since the Minors' Contracts Act doesn't apply to them. I recall that when I went to university aged 17 I had to have a parent sign the contracts, but when I turned 18 I was able to sign them without a parental cosignatory. Neljack (talk) 12:37, 18 November 2013 (UTC)

I apologise for raising such a technical point, but it is what we lawyers are here for, isn't it? :) Neljack (talk) 11:30, 10 November 2013 (UTC)

Oh and while I'm at it I suppose I may as well raise a couple of other unclear points that have just occurred to me. Firstly, would the copy of the ID need to be notarised (by a lawyer, Justice of the Peace, etc)? Secondly, I don't have a government photo ID. What would happen in such cases? Neljack (talk) 11:51, 10 November 2013 (UTC)

Hi Neljack! The age of majority language has been removed from the current draft. Hopefully, that resolves this issue. Mpaulson (WMF) (talk) 23:11, 3 December 2013 (UTC)

> The proposed policy would not need a notarized document, though it would require a government photo ID. We are thinking about proposing another version of this policy, and I guess we could think about adding an alternative identification procedure. What would you suggest? We have also suggested that maybe we simply ditch this policy. What do you think about that? Geoffbrigham (talk) 22:08, 15 November 2013 (UTC)
>
> > There is no government photo ID in the UK as has already been highlighted above along with some alternative suggestions for process. I think by now that a clear majority of unpaid volunteers participating here are concerned or alarmed about the WMF holding onto their ID. Perhaps you would like to see a !vote if that is ambiguous? --Fæ (talk) 03:54, 16 November 2013 (UTC)
> > I think it would be perfectly reasonable for the Foundation to retain the information provided the documents aren't kept, though I have no objection to ditching the policy if that is considered appropriate. As for alternative forms of disclosure, I suppose if somebody required me to prove my identity I would send them a copy of my birth certificate, possibly accompanied by a statutory declaration (witnessed by a Justice of the Peace or lawyer) affirming (on pain of criminal penalties) that it is my certificate. Neljack (talk) 13:09, 18 November 2013 (UTC)
> >
> > > Hi Neljack. The ID requirement has been removed from the current draft of the policy. Thank you for taking the time to share your thoughts on the draft! Mpaulson (WMF) (talk) 23:11, 3 December 2013 (UTC)

Community Committees

The following discussion is closed: ***Closing per comment from Michelle at end. Will archive in a couple days unless reopened. Jalexander--WMF 18:38, 11 December 2013 (UTC)***

Hi, as an OTRS administrator, I would be affected by the policy proposal since it stipulates several changes to the identification procedure. As an affected user, I would like to emphasize a point others have already raised (embedded in wider critiques), which, to me, is by far the most disturbing aspect of the policy proposal. According to the proposed text of the access to nonpublic information policy (henceforth "Policy"), "[s]ometimes, the Wikimedia Foundation or a user community committee will need to contact a community member who formerly had access rights about his or her usage of those rights. For example, the Arbitration Committee may need to complete an ongoing case they are examining [...]" I would like to express my strong opposition to this. As I cannot conceive of any legal reason that would require a disclosure to a "community committee," I am puzzled as to why the Wikimedia Foundation would consider that a necessary or, for that matter, acceptable use of my data.

First, it does not fit into the overall approach of the Policy. At least members of the Election Committee and OTRS administrators do not in their respective roles participate in community processes on individual Wikimedia Wikis. It is therefore not plausible that identifying information about members of either group is passed to community committees for undoubtedly they have no competence to investigate issues that arise within the affected users' capacity as members of these groups in first place. The passing of identifying information about members of these groups to community committees can never serve to fulfill the explicit intent of the identification process ("This helps to increase accountability and ensure against misuse of information entrusted to community members with access to nonpublic information."): Whenever identifying information about such member is provided to a community committee, that must necessarily be related to a member's action unrelated to their treatment of nonpublic information; this cannot be in the spirit of the Policy.

Second, the term/phrase "community committee" is not defined in the Policy and, as far as I am aware, not elsewhere. As of now, the German-language Wikipedia's adaption of the English Wikipedia's Arbitration Committee (the *Schiedsgericht)* does not require members to be identified to the Foundation, and the scope of the two committees' activities differs considerably. Furthermore, there are ad-hoc committees for certain tasks, such as evaluating contests or organizing local elections. In light of this, it is not possible for me to understand, based on the Policy, which "committees" qualify as "community committees" within the meaning of the Policy.

Third, it is not possible at a reasonable effort for members of affected user groups to assess the risk of an undesired use of identifying data by community committees. The Wikimedia Foundation is committed to certain goals and ideals and also has a history of being transparent about internal staff policies. When a member of an affected user group releases identifying information to the Foundation, they can place some trust in the Foundation to process/store/use the information in a responsible manner. They can also keep track of the development of the Foundation and decide if they still desire to provide the Foundation with the identifying information. However, it is entirely impossible to keep track of changes to the composition or policies of community committees in hundreds of Wikimedia Wikis. If a community committee on the Italian-language Wikipedia requests identifying information about me from the Foundation and the Foundation provides the information (be it justified or not), the identifying information gets into the hands of users unknown to me and potentially unknown to the Foundation, residing somewhere in the world. This is unacceptable. Under the current phrasing, providing the Foundation with identifying information is tantamount to providing it with the competence to provide it to third parties effectively free to use the information for purposes other than those envisaged in this Policy. — Pajz (talk) 16:48, 16 October 2013 (UTC)

1. +1 There is a long history of issues with emails sent with an expectation of remaining private or confidential later being released or leaked without permission one way or another when managed by community controlled lists and archives. This does not inspire confidence for how identifying private records would be respected under this policy and the systems being proposed. --Fæ (talk) 16:10, 18 October 2013 (UTC)
2. strong +1 as well. Why would personal information about an OTRS member be disclosed to community members often anonymous. That escapes me. Anthere (talk)

Hi Pajz, Fae, and Anthere! I fear there has been a miscommunication. WMF would not disclose information from the submitted identification documents to other volunteers. Under the applicable clause in this draft, "The Wikimedia Foundation will not share submitted materials with third parties, unless such disclosure is (A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department; (B) required by law; (C) needed to protect against immediate threat to life or limb; or (D) needed to protect the rights, property, or safety of the Wikimedia Foundation, its employees, or contractors." The text in the subsection following stating: "Sometimes, the Wikimedia Foundation or a user community committee will need to contact a

community member who formerly had access rights about his or her usage of those rights. For example, the Arbitration Committee may need to complete an ongoing case they are examining or the Wikimedia Foundation may need to notify you of receipt of a legal document involving that community member." is not meant to say that we would disclose the identifying information about you to other community members. This section was meant to explain the reasons for retention of your identification information. WMF would not give your identification information to other community members in this situation. We would contact you using the information you submitted to us to let you know that ArbCom needs to get ahold of you regarding an ongoing case. Would clarifying that in the policy draft help? We could also get rid of that portion talking about community committees and ArbCom all together if it's too confusing. What do you think? Mpaulson (WMF) (talk) 18:55, 31 October 2013 (UTC)

> Perhaps adding another sentence like "In that scenario, the WMF would notify you through the information you provided to us about this, but your contact information would not be given to the community members"? --**Rschen7754** 19:05, 31 October 2013 (UTC)
>
> Yes, you do need to clarify the wording. My English comprehension has been tested as excellent, even for a native speaker, so reading this again tells me that under section D, the WMF is free to share any information it wishes with any (unnamed) third party to protect its property or rights. In legal parlance, the unqualified terms "property" and "rights" are so wide as to accommodate virtually anything, including weird stuff of potential rather than defined value like reputation of the Wikimedia projects or the WMF "brand", disputed domain name registrations, or disputed claims of copyright of its materials or future "community logos". To emphasise the point, "third parties" means *anyone*. --Fæ (talk) 19:25, 31 October 2013 (UTC)
>
> Dear Michelle, thank you for your detailed response. I would certainly appreciate a clarification in the draft, though I am indifferent as to whether that should take the form of a removal of the passage about community committees alltogether or a rephrasing in the spirit of Rschen7754's proposal above; as for me, I cannot conceive of a reason why a community committee would need to reach identified users through these means. If a user is ready to answer questions from community committees, they won't have a problem reaching him; if he does not leave contact information and does not react to posts on his talk page, odds are that he just doesn't wish to be involved in Wikipedia or Wikimedia matters anymore. And while these committees play a vital role in our community, they are not ultimately conducting legally relevant investigations, so why bother identified volunteers? But as I said, I don't really care about that as long as the Foundation doesn't pass the information to members of these committees.
> Which brings me to another passage you quote, and which Fae criticizes above. I concur with Fae's point. I'm not happy with (D) in its current form. As Fae points out, the provision is lacking any specification of the third party involved. I am sure you have given this more thought than I have, but couldn't this at least be narrowed down to law enforcement agencies? In another comment of yours, you suggest to change the wording from "(D) needed to protect the rights, property, or safety of the Wikimedia Foundation, its employees, or contractors" to "(D) needed to protect the safety of others or WMF staff, contractors, systems or property" and give the example of an identified community member breaking into your building. Earlier today, you provided another example of a volunteer who "purposefully planted any viruses, malware, worms, Trojan horses, or malicious code that could harm our technical infrastructure in violation of the Terms of Use or that could expose the personal, nonpublic information of other users." In both cases I assume that the party you would share the information with is a police agency and/or a state attorney (I presume this varies among different legal systems). This suggests to me that you could narrow down the third party recipients of the information as proposed. I do have some other criticism with respect to the points (A)–(D), but I do think that a specification of "third party" would be a grave improvement anyway. I would be interested in your thoughts on this. Regards, — Pajz (talk) 23:01, 31 October 2013 (UTC)
>
> > Hi Pajz. I understand your concern regarding the term "third party" in relation to subsection (D)(i). We are currently reevaluating that section in light of community feedback and will be responding accordingly in a thread below. Because the community committees topic has been resolved, we are going to close this thread and continue the discussion about which scenarios sharing submitted materials would be appropriate in the other thread. Thank you for your feedback and patience! Mpaulson (WMF) (talk) 00:17, 10 December 2013 (UTC)

Retrieved from "https://meta.wikimedia.org/w/index.php?title=Talk:Access_to_nonpublic_information_policy/Archives/2013&oldid=16362352"

This page was last edited on 26 February 2017, at 17:57.

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. See Terms of Use for details.

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

Plaintiff's Exhibit 10

OTRS Open Technology Real Services

Redacted

Global exception request

printed by James Alexander (jalexander@wikimedia.org), 04/11/2018 21:49:27

State	closed successful	**Age**	1661 d 10 h
Priority	3 normal	**Created**	09/23/2013 11:06:06
Queue	stewards		
Lock	lock		
CustomerID	Redacted@wikimedians.ca		
Owner	Jamesofur (James Alexander)		

Article #1

From: Redacted @wikimedians.ca>
To: stewards@wikimedia.org
Subject: Global exception request
Created: 09/23/2013 11:06:06 by customer
Type: email-external

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Hi! I was referred to meta[1] when I whinged about not being able to
edit from my currently-preferred browser, which utilizes TOR amongst
other privacy precautions.

I am a US citizen living abroad. According to recent news reports this
places me in a category for elevated surveillance by my government,
despite such surveillance of its citizens actually being illegal under
US law. I prefer to minimize such invasions of my privacy and so use
TOR where possible. The global block on TOR exit points has reduced my
spontaneous contributions to the WMF projects I am still somewhat
involved with. I believe I would contribute more if, when I see
something to fix, I could simply log in and edit rather than log in,
attempt to edit, get told I'm blocked, load a different browser and
navigate to the page I wish to edit, log in again, and finally make
the change.

I believe I am a wikimedian in good standing, with a moderate history
of involvement with WMF and with the WMF projects, and am unlikely to
engage in grossly inappropriate behaviour (other than, perhaps,
discussions regarding WMF trademark practices.)

Regards,

Redacted

P.S. Oh, I'm Redacted everywhere... obviously it's the username I'd
prefer to use (and if any of you would be willing to just usurp that
darned Italian login I made waaaaaaaay long time ago so I could
finally achieve SUL, I'd appreciate that, too. Yah, I've tried to get
it through the it.WP bureaucrats a couple of times.)

[1]
https://meta.wikimedia.org/wiki/No_open_proxies#Global_exceptions_and_appeals
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.12 (GNU/Linux)
Comment: Using GnuPG with Thunderbird - http://www.enigmail.net/

Redacted
-----END PGP SIGNATURE-----
```

Article #2

From: Wikimedia stewards <stewards@wikimedia.org>
To: Redacted@wikimedians.ca
Subject: Re: [Ticket# Redacted] Global exception request
Created: 09/23/2013 11:17:20 by agent
Type: email-external

OTRS Open Technology Real Services

Redacted

Gday Redacted

Did the global IP block exemption.

Re the account, when they do their global account reconciliation you will get the global account and the other will be renamed, so leaving it and letting it happen is the best management means.

Regards, sDrewth

Wikimedia Stewards

Disclaimer: all mail to this address is answered by volunteers, and responses are not to be considered an official statement of the Wikimedia Foundation. For official correspondence, please contact the Wikimedia Foundation by certified mail at the address listed on <https://www.wikimediafoundation.org/>

23/09/2013 11:06 - Redacted wrote:

> -----BEGIN PGP SIGNED MESSAGE-----
> Hash: SHA1
>
> Hi! I was referred to meta[1] when I whinged about not being able to
> edit from my currently-preferred browser, which utilizes TOR amongst
> other privacy precautions.
>
> I am a US citizen living abroad. According to recent news reports this
> places me in a category for elevated surveillance by my government,
> despite such surveillance of its citizens actually being illegal under
> US law. I prefer to minimize such invasions of my privacy and so use
> TOR where possible. The global block on TOR exit points has reduced my
> spontaneous contributions to the WMF projects I am still somewhat
> involved with. I believe I would contribute more if, when I see
> something to fix, I could simply log in and edit rather than log in,
> attempt to edit, get told I'm blocked, load a different browser and
> navigate to the page I wish to edit, log in again, and finally make
> the change.
>
> I believe I am a wikimedian in good standing, with a moderate history
> of involvement with WMF and with the WMF projects, and am unlikely to
> engage in grossly inappropriate behaviour (other than, perhaps,
> discussions regarding WMF trademark practices.)
>
> Regards,
>
> Redacted
>
> P.S. Oh, I'm Redacted everywhere... obviously it's the username I'd
> prefer to use (and if any of you would be willing to just usurp that
> darned Italian login I made waaaaaaaay long time ago so I could
> finally achieve SUL, I'd appreciate that, too. Yah, I've tried to get
> it through the it.WP bureaucrats a couple of times.)
>
> [1]
> https://meta.wikimedia.org/wiki/No_open_proxies#Global_exceptions_and_appeals
> -----BEGIN PGP SIGNATURE-----
> Version: GnuPG v1.4.12 (GNU/Linux)
> Comment: Using GnuPG with Thunderbird - http://www.enigmail.net/
>
> Redacted
> -----END PGP SIGNATURE-----
>
>

Article #3

From:	Wikimedia stewards <stewards@wikimedia.org>
To:	apalmer@wikimedia.org
Subject:	Fwd: [Ticket# Redacted] Global exception request
Created:	04/03/2018 23:24:05 by agent
Type:	email-external

Yours sincerely,
James Alexander

Wikimedia Stewards

Disclaimer: all mail to this address is answered by volunteers, and responses are not to be considered an official statement of the Wikimedia Foundation. For official correspondence, please contact the Wikimedia Foundation by certified mail at the address listed on <https://www.wikimediafoundation.org/>
---- Forwarded message from Redacted @wikimedians.ca> ---

From: Redacted @wikimedians.ca>

OTRS Open Technology Real Services

Redacted

To: stewards@wikimedia.org
Subject: Global exception request
Date: 09/23/2013 11:06:06

> -----BEGIN PGP SIGNED MESSAGE-----
> Hash: SHA1
>
> Hi! I was referred to meta[1] when I whinged about not being able to
> edit from my currently-preferred browser, which utilizes TOR amongst
> other privacy precautions.
>
> I am a US citizen living abroad. According to recent news reports this
> places me in a category for elevated surveillance by my government,
> despite such surveillance of its citizens actually being illegal under
> US law. I prefer to minimize such invasions of my privacy and so use
> TOR where possible. The global block on TOR exit points has reduced my
> spontaneous contributions to the WMF projects I am still somewhat
> involved with. I believe I would contribute more if, when I see
> something to fix, I could simply log in and edit rather than log in,
> attempt to edit, get told I'm blocked, load a different browser and
> navigate to the page I wish to edit, log in again, and finally make
> the change.
>
> I believe I am a wikimedian in good standing, with a moderate history
> of involvement with WMF and with the WMF projects, and am unlikely to
> engage in grossly inappropriate behaviour (other than, perhaps,
> discussions regarding WMF trademark practices.)
>
> Regards,
>
> Redacted
>
> P.S. Oh, I'm Redacted everywhere... obviously it's the username I'd
> prefer to use (and if any of you would be willing to just usurp that
> darned Italian login I made waaaaaaaay long time ago so I could
> finally achieve SUL, I'd appreciate that, too. Yah, I've tried to get
> it through the it.WP bureaucrats a couple of times.)
>
> [1]
> https://meta.wikimedia.org/wiki/No_open_proxies#Global_exceptions_and_appeals
> -----BEGIN PGP SIGNATURE-----
> Version: GnuPG v1.4.12 (GNU/Linux)
> Comment: Using GnuPG with Thunderbird - http://www.enigmail.net/
>
> Redacted
> -----END PGP SIGNATURE-----
>
>
---- End forwarded message ---

HIGHLY PROTECTED – ATTORNEYS' EYES ONLY FOIA Confidential Treatment Request