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 5 OF 7 (JA2890–JA3406)

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

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

Plaintiff's Exhibit 22

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

GOVERNMENT'S RESPONSE TO THE COURT'S BRIEFING ORDER OF MAY 9, 2011

1. The government's May 2 Letter can be read to take the position that [redacted] are communications authorized for collection under the Section 702 Certifications that have previously been approved by the Court. ~~(TS//SI//NF)~~

a. For how long has NSA been acquiring [redacted] through its upstream collection? ~~(TS//SI//NF)~~

Under the Section 702 Certifications, NSA acquires, *inter alia*, "Internet communications." *E.g.*, DNI/AG 702(g) Certification [redacted], Affidavit of General Keith B. Alexander, Director, National Security Agency (NSA), filed Apr. 20, 2011, at ¶ 4. As described by General Alexander, Internet communications "include, but are not limited to, [redacted] *E.g.*, *id.* ~~(TS//SI//NF)~~

In the context of NSA's upstream collection techniques, NSA acquires Internet communications in the form of "transactions," which in this filing refers to a complement of "packets" traversing the Internet that together may be understood by a device on the Internet and, where applicable, rendered in an intelligible form to the user of that device.[1] A "transaction" might contain information or data representing either a discrete communication (e.g., an e-mail message), or multiple discrete communications [redacted]. As further described in the response to question 2 below, whenever a tasked selector is present within a transaction, NSA's "upstream" Internet collection techniques are designed to identify and acquire that transaction. ~~(TS//SI//NF)~~

[1] While the terms "Internet communication" and "transmission" have been used to describe the types of communications NSA acquires, NSA believes that, in the context of upstream collection, "transaction" is the more precise term from a technical perspective, because "transmission" could be understood to mean all data being exchanged on the Internet within a specific time period by a specific device, and an "Internet communication" may actually contain multiple logically separate communications between or among persons. ~~(TS//SI//NF)~~

The transactions discussed herein -- whether they contain single or multiple discrete communications having a commonality of a single user -- should not be confused with the two [redacted] compliance incidents initially reported to the Court on April 19, 2011, and further discussed below in the Government's response to question 6, which involved the [redacted] unrelated communications [redacted] ~~(TS//SI//NF)~~

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20360501

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

At the time of acquisition, NSA's upstream Internet collection devices are, with limited exceptions further described below, not presently capable of distinguishing transactions containing only a single discrete communication to, from, or about a tasked selector from transactions containing multiple discrete communications, not all of which may be to, from, or about a tasked selector.[2] Thus, in order to acquire transactions containing one or more communications to, from, or about a tasked selector, it has been necessary for NSA to employ these same upstream Internet collection techniques throughout the entire timeframe of all certifications authorized under Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (hereinafter "FISA" or "the Act"), and the Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (Aug. 5, 2007) (hereinafter "PAA"). It was also necessary for NSA to employ these upstream collection techniques to implement the electronic surveillance authorized in *In re* [redacted] Docket No. [redacted] and *In re* [redacted] Docket No. [redacted] ~~(TS//SI//NF)~~

b. **According to the May 2 Letter, [redacted] may include the full content of email messages that are not to, from or about the user of a targeted selector. They also may include discrete communications as to which all communicants are within the United States. Please explain how the acquisition of such transmissions: ~~(TS//SI//NF)~~**

i. **comports with the government's representations to the Court regarding the scope of upstream collection under Section 702 and the approvals granted by the Court in reliance upon those representations in Dockets 702(i) 08-01, [redacted] (see, e.g., Docket No. 702(i)-08-01, Aug. 27, 2008 Hearing Transcript at 19-26, 40-41 and Sept. 4, 2008 Memorandum Opinion at 15-20, 38); ~~(TS//SI//NF)~~**

The Government has concluded, after a careful review of the record, that its prior representations to the Court regarding the steps NSA must take in order to acquire single, discrete communications to, from, or about a tasked selector did not fully explain all of the means by which such communications are acquired through NSA's upstream collection techniques. The Government will attempt through this filing to provide the Court with a more thorough explanation of this technically complex collection. This notwithstanding, the Government respectfully submits that for the reasons set forth in its responses to questions 2.ii.,

[2] Specifically, as is discussed in the Government's response to questions 2(c) and (d) of the Court's briefing order, NSA does have the ability to identify and acquire discrete communications to, from, or about a tasked selector in certain cases [redacted] ~~(TS//SI//NF)~~

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

2.iii., and 5 below, NSA's prior and ongoing acquisition of information utilizing its upstream collection techniques is consistent with the Court's prior orders, meets the requirements of Section 702, and is consistent with the Fourth Amendment. ~~(TS//SI//NF)~~

b. **According to the May 2 Letter, [redacted] may include the full content of email messages that are not to, from or about the user of a targeted selector. They also may include discrete communications as to which all communicants are within the United States. Please explain how the acquisition of such transmissions: ~~(TS//SI//NF)~~**

ii. **meets the requirements of Section 702, including, but not limited to, the requirement that targeting procedures must be reasonably designed to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States"; and, ~~(TS//SI//NF)~~**

NSA'S TARGETING PROCEDURES ARE REASONABLY DESIGNED TO PREVENT THE INTENTIONAL ACQUISITION OF COMMUNICATIONS AS TO WHICH THE SENDER AND ALL INTENDED RECIPIENTS ARE KNOWN AT THE TIME OF ACQUISITION TO BE LOCATED IN THE UNITED STATES. ~~(S)~~

Under Section 702, the Government targets "persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a). The Government determines whether the targeting of a person is consistent with Section 702 by applying Court-approved targeting procedures. 50 U.S.C. § 1881a(d). These targeting procedures must be "reasonably designed to (A) ensure that any acquisition authorized under subsection [702(a)] is limited to targeting persons reasonably believed to be located outside the United States; and (B) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States." 50 U.S.C. § 1881a(d)(1). (U)

A. The User of a Tasked Selector is the Person Being Targeted by all Acquisitions by NSA's Upstream Collection, Including Transactions That Contain Multiple Discrete Communications ~~(TS//SI//NF)~~

As previously explained to the Court, the Government "targets" a person by tasking for collection a "selector" (e.g., an e-mail account) believed to be used by that person. *See, e.g., In re DNI/AG Certification* [redacted] Docket No. 702(i)-08-01, Mem. Op. at 8 (USFISC Sept. 4, 2008) (hereinafter "[redacted] Mem. Op."). NSA acquires foreign intelligence information through the tasking of selectors by collecting communications to or from a selector used by a targeted person (hereinafter "to/from communications") and by collecting communications that refer to or are about a selector used by a targeted person (hereinafter "abouts communications"). *Id.* ~~(TS//SI//NF)~~

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

In both of these types of acquisition, the person being "targeted" is the user of the tasked selector, who, by operation of the targeting procedures, is a non-United States person reasonably believed to be located outside the United States. Specifically, "the persons targeted by acquisition of to/from communications are the users of the tasked selectors," because "their communications are intentionally selected for acquisition." [redacted] Mem. Op. at 15. Similarly, the person being targeted by acquisition of abouts communications is also the user of the tasked selector, "because the government's purpose in acquiring about communications is to obtain information about that user." *Id.* at 18 (citation omitted). ~~(TS//SI//NF)~~

This remains true for all acquisitions conducted by NSA's upstream collection -- including transactions containing several discrete communications, only one of which may be to, from, or about the user of a tasked selector. As discussed above, the fact that there also may be communications to, from, or about persons other than the target in the transaction does not mean that those persons are also being targeted by the acquisition. The sole reason a transaction is selected for acquisition is that it contains the presence of a tasked selector used by a person who has been subjected to NSA's targeting procedures.[3] Indeed, at the time a transaction is acquired, NSA cannot always know whether the transaction includes other data or information representing communications that are not to, from, or about the target, let alone always have knowledge of the parties to those communications. *Cf.* [redacted] Mem. Op. at 18-19 (noting that with respect to abouts communications, "the government may have no knowledge of [the parties to a communication] prior to acquisition"). It therefore cannot be said that the acquisition of a transaction containing multiple discrete communications results in the intentional targeting of any of the parties to those communications other than the user of the tasked selector. *Cf. United States v. Bin Laden*, 126 F. Supp. 2d 264, 281 (S.D.N.Y. 2000), *aff'd sub nom. In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 157 (2d Cir. 2008), *cert. denied sub nom. El-Hage v. United States*, 130 S.Ct. 1050 (2010) (acknowledging that in light of *United States v. Verdugo-Urquidez*, 494 U.S. 259, 265 (1990), and Title III "incidental interception" case law, overseas surveillance of a United States person terrorism suspect would have posed no Fourth Amendment problem "if the Government had not been aware of [his] identity or of his complicity in the [terrorism] enterprise"). ~~(TS//SI//OC,NF)~~

[redacted]

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

B. NSA's Targeting Procedures are Reasonably Designed to Prevent the Intentional Acquisition of Communications as to Which the Sender and All Intended Recipients Are Known at the Time of Acquisition to be in the United States ~~(S)~~

In conducting acquisitions targeting the user of a tasked selector, the Government "may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States." 50 U.S.C. § 1881a(b)(4). As noted above, the targeting procedures must be reasonably designed to prevent such intentional acquisitions. With respect to to/from communications, "because a user of a tasked selector is a party to every to/from communication acquired by NSA, a reasonable belief that the users of tasked selectors are outside the United States will ensure that NSA does not intentionally acquire any to/from communication 'as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States.'" [redacted] Mem. Op. at 15 (citation omitted). With respect to upstream collection that may contain abouts communications, NSA's targeting procedures provide that:

[redacted][4]

E.g., Amendment 1 to DNI/AG 702(g) Certification [redacted] Docket No. 702(i)-[redacted] Ex. A, filed Aug. 12, 2010, at 1-2 (hereinafter "NSA Targeting Procedures"). Although these provisions on their face suggest separate technical means might apply only to the "abouts" aspect of NSA's upstream collection, in practice these provisions currently apply to any Internet transaction collected upstream. ~~(TS//SI//OC,NF)~~

The Government has previously represented that "the operation of the IP address filters or [redacted] prevents the intentional acquisition of communications 'about' the target as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States." *In re DNI/AG 702(g) Certification* [redacted] Docket No. 702(i)-08-01, Government's Preliminary Response to Questions Posed by the Court, filed Aug. 26, 2008, at 3. The Government also has represented that these IP filters "have been effective in limiting the collection to communications with at least one communicant located outside the United States."

[4] This provision has remained identical throughout every set of NSA's Section 702 targeting procedures approved for use by the Court, and is also the same in the proposed targeting procedures submitted with DNI/AG 702(g) Certifications [redacted] ~~(S//OC,NF)~~

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

Id. at 4. Except in one circumstance previously reported to the Court,[5] the Government is not aware of a case where an about collection resulted in the acquisition of a communication where both ends were inside the United States. NSA therefore continues to believe that these prior representations remain accurate. Accordingly, for the reasons described below, the Government respectfully submits that NSA's targeting procedures are reasonably designed to prevent, in the context of NSA's upstream collection, "the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States," including Internet communications [redacted] that have not been previously described to the Court. 50 U.S.C. § 1881a(d)(1)(B). ~~(TS//SI//OC,NF)~~

1. How NSA's IP Filters Work ~~(S)~~

NSA acquires Internet communications by collecting the individual packets of data that make up those communications. [redacted]

~~(TS//SI//OC,NF)~~ [redacted]

[5] [redacted] ~~(TS//SI//NF)~~

[6] [redacted] ~~(TS//SI//NF)~~

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

[redacted] ~~(TS//SI//OC,NF)~~

[redacted]

Additionally, at the time of acquisition, NSA's upstream Internet collection devices are, with limited exceptions further described below, not presently capable of distinguishing transactions containing only a single discrete communication to, from or about a targeted selector from transactions containing multiple discrete communications.[7] Accordingly, NSA cannot prevent the acquisition of, or even mark for separate treatment, those types of transactions that may feature multiple discrete communications [redacted]. ~~(TS//SI//OC,NF)~~

[redacted]

[7] *See* Government's response to questions 2(c) and (d) *infra*. (U)

[redacted] ~~(TS//SI//NF)~~

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

[redacted]

[redacted][10] ~~(TS//SI//OC,NF)~~

Except for the one instance noted above concerning an error by an electronic communication service provider, NSA is not aware of any instance in which its upstream collection on [redacted] or are subject to an IP filter nevertheless resulted in the acquisition of a communication as to which the sender and all intended recipients were known at the time of acquisition to be located in the United States.[11] This includes those situations in which NSA might collect unrelated communications when acquiring Internet communications that include multiple, discrete communications. ~~(TS//SI//NF)~~

[redacted]

~~(TS//SI//OC,NF)~~

[redacted]

[redacted] ~~(TS//SI//OC,NF)~~

[11] It is noteworthy that the provider error that resulted in the acquisition of domestic communications was first identified not by the provider, but by an NSA analyst who recognized a domestic communication in NSA's repositories, realized that such a domestic communication should not have been acquired, and properly reported the communication through NSA channels. NSA investigated this matter and found that domestic communications had been acquired not due to any theoretical limitations in its IP filter technology, but instead because [redacted] The domestic overcollection caused by this incident represented a very small portion of NSA's collection during the time period of the overcollection, and an even smaller portion of NSA's collection since the initiation of its Section 702 acquisitions, but the error was still discovered and remedied. It is therefore particularly noteworthy that no NSA analyst has otherwise yet discovered a wholly domestic communication in NSA's repositories collected through NSA's upstream collection systems. ~~(TS//SI//OC,NF)~~

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

In May 2011, NSA conducted two tests of its Section 702 upstream collection in order to determine the likelihood of collecting an Internet transaction between a user in the United States and [redacted] The first test included [redacted]

The second test included [redacted]

~~(TS//SI//NF)~~

The first test sample included no records where both the sender and receiver IP addresses were in the United States [redacted] NSA analysis further revealed that only [redacted] of the more than [redacted] (0.0028%) had characteristics consistent with a person in the United States accessing a [redacted] For the second dataset, NSA analysis discovered that only [redacted] out of more than [redacted] total records (0.0016%) included a non-targeted user likely accessing the Internet from an IP address in the United States. [redacted] NSA assesses, based on analysis of the underlying data, that this activity in fact was [redacted] copies of the same Internet transaction, [redacted] There is no indication that NSA collected any wholly domestic communications through its acquisition of this transaction. ~~(TS//SI//NF)~~

In sum, the Government submits that the two test samples discussed above, coupled with the fact that, except as noted above, no NSA analyst has yet discovered in NSA's repositories a wholly domestic communication collected through NSA's upstream collection systems, strongly suggests that NSA's acquisition of transactions or single Internet communications between users in the United States and [redacted] currently occurs only in a very small percentage of cases. Even those rare cases, moreover, won't necessarily involve a user in the United States receiving from the [redacted] a transaction containing a communication from a person known at the time of acquisition to be located in the United States.[12] ~~(TS//SI//NF)~~

[12] Additionally, as discussed elsewhere herein, even if the sender is located in the United States, the communication likely will not contain any reliable information that would enable NSA to determine at the time of acquisition the sender's location. ~~(TS//SI//OC,NF)~~

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

2. The [redacted] Means by Which NSA Prevents the Intentional Acquisition of Communications as to Which the Sender and All Intended Recipients Are Known to be Located In the United States at the Time of Acquisition Are Reasonable ~~(S)~~

This Court has found that NSA's targeting procedures are reasonably designed to prevent the intentional acquisition of communications in which the sender and all intended recipients are known at the time of acquisition to be located in the United States. In approving DNI/AG 702(g) Certification [redacted], with respect to NSA's upstream collection of "abouts" communications, in particular, the Court noted that NSA "relies on [redacted] means of ensuring that at least one party to the communication is located outside the United States." [redacted] Mem. Op. at 19. As described above, those [redacted] means are NSA's use of "an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas" and NSA's [redacted] NSA Targeting Procedures at 1-2; *see also* [redacted] Mem. Op. at 19. Relying on the Government's representations that these [redacted] means had prevented the acquisition of wholly domestic communications under the PAA, and recognizing that it is "theoretically possible that a wholly domestic communication could be acquired as a result of the [redacted]" the Court found that these [redacted] means were "reasonably designed to prevent the intentional acquisition of communications as to which all parties are in the United States." [redacted] Mem. Op. at 20 & n.17. The Government respectfully submits that there is no aspect of NSA's upstream collection, as further described herein, that would prevent the Court from continuing to find that NSA's targeting procedures are reasonably designed to prevent the intentional acquisition of communications as to which the sender and all intended recipients are known at the time of acquisition to be in the United States. ~~(TS//SI//OC,NF)~~

Two aspects of NSA's upstream collection activity that have not been specifically addressed by the Court are discussed herein: first, the fact that NSA acquires some communications [redacted] and second, the fact that NSA could acquire [redacted] -- whether retrieving a single, discrete communication, or a transaction containing several discrete communications -- possibly resulting in the acquisition of wholly domestic communications. ~~(TS//SI//OC,NF)~~

a. Acquisition of Communications that [redacted] ~~(S)~~

First, [redacted] -- NSA's targeting procedures are reasonably designed to prevent the intentional acquisition of communications as to which the sender and all intended recipients are known at the time of acquisition to be located in the United

NYT v DOJ, 16 CIV 7020_000376
NSA-WIKI 00246

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

States. [redacted] ~~(TS//SI//OC,NF)~~

b. **Theoretical Acquisition of Wholly Domestic Communications Through** [redacted] ~~(TS//SI//NF)~~

With respect to the above-discussed theoretical cases in which NSA could acquire a [redacted] NSA's targeting procedures also are reasonably designed to prevent the intentional acquisition of communications as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States. As discussed above, NSA assesses that [redacted] only in a minute percentage of cases. Yet even in those rare cases, there would be no way for NSA to know at the time of acquisition that the sender and intended recipient are located in the United States. [redacted] NSA cannot at that point know the location of the intended recipient, who has yet to receive the message. Likewise, [redacted] it is highly unlikely that the communication would contain information useful in determining the sender's true location.[13] In any event, it is currently not possible for NSA's IP filters to [redacted] Because NSA's filters will be looking at the best available information, [redacted] it cannot be said that the sender and all intended recipients of those communications are known at the time of acquisition to be located in the United States. Similarly, in the case of NSA's [redacted]

[13] [redacted] ~~(TS//SI//OC,NF)~~

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

[redacted] ~~(TS//SI//OC,NF)~~

Accordingly, NSA has designed its systems so that it should never intentionally acquire a communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States. To the extent that NSA does unintentionally acquire such communications, NSA must treat those communications in accordance with its minimization procedures -- just as it must for other types of communications that it is prohibited from intentionally collecting under subsection 702(b), but nevertheless sometimes does unintentionally acquire, such as communications acquired from a target while that target is located inside the United States. ~~(TS//SI//OC,NF)~~

c. Conclusion (U)

Although for different reasons than those discussed above, the Court has recognized that it is "theoretically possible that a wholly domestic communication could be acquired" through NSA's upstream collection of "abouts" communications. [redacted] Mem. Op. at 20 n.17. For the reasons outlined above, the Government respectfully submits that, despite the theoretical scenarios under which NSA could acquire communications through its upstream collection as to which the sender and all intended recipients are located in the United States, NSA's targeting procedures are reasonably designed to prevent such acquisitions where the location of the sender and all intended recipients is known at the time of acquisition. ~~(TS//SI//OC,NF)~~

The remainder of this page intentionally left blank.

Approved for public release, All withheld information exempt under b(1) and b(3) except as otherwise noted.

b. **According to the May 2 Letter, [redacted] may include the full content of email messages that are not to, from or about the user of a targeted selector. They also may include discrete communications as to which all communicants are within the United States. Please explain how the acquisition of such transmissions:** ~~(TS//SI//NF)~~

iii. is consistent with the Fourth Amendment. ~~(TS//SI//NF)~~

NSA's ACQUISITION OF TRANSACTIONS CONTAINING MULTIPLE DISCRETE COMMUNICATIONS IS CONSISTENT WITH THE FOURTH AMENDMENT. (TS//SI//NF)

Section 702 requires the Attorney General (AG) and the Director of National Intelligence (DNI) to execute a certification attesting, among other things, that the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment. 50 U.S.C. § 1881a(g)(2)(A)(iv). In reviewing a certification, Section 702 in turn requires the Court to enter an order approving the certification and the use of the targeting and minimization procedures if the Court finds, among other things, that those procedures are consistent with the requirements of the Fourth Amendment. *Id.* § 1881a(i)(3)(A). The issue for the Court in light of the above-described nature and scope of NSA's upstream collection is whether, in light of a governmental interest "of the highest order of magnitude," NSA's targeting and minimization procedures sufficiently protect the individual privacy interests of United States persons whose communications are inadvertently acquired. *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1012 (Foreign Int. Surv. Ct. Rev. 2008) (hereinafter "*In re Directives*"). ~~(TS//SI//NF)~~

The Fourth Amendment protects the right "to be secure . . . against unreasonable searches and seizures" and directs that "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." U.S. Const. amend. IV. As demonstrated below, the Fourth Amendment requires no warrant here, and the upstream collection conducted by NSA is a reasonable exercise of governmental power that satisfies the Fourth Amendment. ~~(TS//SI//NF)~~

A. The Warrant Requirement Does Not Apply to NSA's Acquisition of Transactions Containing Multiple Discrete Communications. ~~(TS//SI//NF)~~

The Supreme Court has recognized exceptions to the Fourth Amendment's warrant requirement "when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987) (internal quotations omitted); *see also Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995) (quoting *Griffin*). The Foreign Intelligence Surveillance Court of Review, in upholding the Government's implementation of the PAA, held that a foreign intelligence exception exists "when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

believed to be located outside the United States." *In re Directives*, 551 F.3d at 1012. *See also In re Sealed Case*, 310 F.3d 717, 742 (Foreign Int. Surv. Ct. Rev. 2002) ("[A]ll the . . . courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information."). ~~(TS//SI//NF)~~

In approving a previous Section 702 certification, this Court has found that Section 702 acquisitions "fall within the exception recognized by the Court of Review" in that they "target persons reasonably believed to be located outside the United States who will have been assessed by NSA to possess and/or to be likely to communicate foreign intelligence information concerning a foreign power authorized for acquisition under the Certification" and are "conducted for national security purposes." [redacted] Mem. Op. at 35 (citations omitted). Specifically, this Court recognized that the Court of Review's rationale for applying a foreign intelligence exception "appl[ies] with equal force" to Section 702 acquisitions, in that the Government's purpose in conducting Section 702 acquisitions goes well beyond a normal law enforcement objective and involves "'the acquisition from overseas foreign agents of foreign intelligence to help protect national security,' a circumstance in which the government's interest is particularly intense.'" *Id.* at 35-36 (quoting *In re Directives*, 551 F.3d at 1011). In addition, this Court, noting the likely volume of Section 702 acquisitions and the fact that those acquisitions involve targets who are attempting to conceal their communications, found that "[s]ubjecting [redacted] number of targets to a warrant process inevitably would result in delays and, at least occasionally, in failures to obtain perishable foreign intelligence information, to the detriment of national security." [redacted] Mem. Op. at 36; *see also United States v. Truong Dinh Hung*, 629 F.2d 908, 913 (4th Cir. 1980) ("attempts to counter foreign threats to the national security require the utmost stealth, speed, and secrecy" such that "[a] warrant requirement would add a procedural hurdle that would reduce the flexibility of executive foreign intelligence initiatives, [and] in some cases delay executive response to foreign intelligence threats..."). The Court's previous finding that the foreign intelligence exception applies to Section 702 acquisitions remains equally applicable here. ~~(TS//SI//NF)~~

B. NSA's Acquisition of Transactions Containing Multiple Discrete Communications is Reasonable Under the Fourth Amendment. ~~(TS//SI//NF)~~

Where, as here, the foreign intelligence exception applies, "governmental action intruding on individual privacy interests must comport with the Fourth Amendment's reasonableness requirement." *In re Directives*, 551 F.3d at 1012. In evaluating the reasonableness of the Government's action, a court must consider the totality of the circumstances, *see United States v. Knights*, 534 U.S. 112, 118 (2001), taking into account "the nature of the government intrusion and how the intrusion is implemented." *In re Directives*, 551 F.3d at 1012 (citing *Tennessee v. Garner*, 471 U.S. 1, 8 (1985) and *United States v. Place*, 462 U.S. 696, 703 (1983)). In balancing these interests, the Court of Review has observed that "[t]he more important the government's interest, the greater the intrusion that may be constitutionally tolerated." *In re Directives*, 551 F.3d at 1012 (citing *Michigan v. Summers*, 452 U.S. 692, 701-05 (1981)). "If the protections that are in place for individual privacy interests are sufficient in light of the governmental interests at stake, the constitutional scales will tilt in favor of upholding the government's actions." *Id.* ~~(TS//SI//NF)~~

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

1. NSA's Acquisition of Transactions Containing Multiple Discrete Communications Implicates Fourth Amendment-Protected Interests. ~~(TS//SI//NF)~~

Although targeting under Section 702 is limited to non-United States persons reasonably believed to be located outside the United States, who are not entitled to protection under the Fourth Amendment, *see, e.g.,* [redacted] Mem. Op. at 37, this Court has recognized that conducting acquisitions under Section 702 creates a "real and non-trivial likelihood of intrusion on Fourth Amendment-protected interests" of United States persons or persons located in the United States who, for example, communicate directly with a Section 702 target, *id.* at 38.[14] In particular, as described herein, NSA's upstream collection may incidentally acquire information concerning United States persons within transactions containing multiple discrete communications, only one of which is to, from, or about a person targeted under Section 702. ~~(TS//SI//NF)~~

2. The Government's Interest in the Foreign Intelligence Information Contained in All Transactions, Including Those Containing Multiple Discrete Communications, is Paramount. ~~(TS//SI//NF)~~

On the other side of the ledger, it is axiomatic that the Government's interest in obtaining foreign intelligence information to protect the Nation's security and conduct its foreign affairs is paramount. *See, e.g., Haig v. Agee*, 453 U.S. 280, 307 (1981) ("[I]t is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation." (citations omitted)). Equally indisputable is the Government's interest in conducting acquisitions of foreign intelligence information[15] under Section 702 of the Act. *See* [redacted] Mem. Op. at 37

[14] Although the scope of Fourth Amendment protection for e-mail is not settled, the Government has argued before this Court that United States persons have a reasonable expectation of privacy in the content of such electronic communications. *See, e.g.*, United States of America's Supplemental Brief on the Fourth Amendment, Docket No. 105B(g) 07-01, filed Feb. 15, 2008, at 1. The Government likewise assumes for purposes of this filing that the collection of [redacted] implicates privacy interests protected by the Fourth Amendment. ~~(TS//SI//NF)~~

[15] "Foreign intelligence information" is defined as:

(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.

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

("The government's national security interest in conducting these acquisitions 'is of the highest order of magnitude.'" (quoting *In re Directives*, 551 F.3d at 1012)). For example,

[redacted] ~~(TS//SI//NF)~~

The Supreme Court has indicated that in addition to examining the governmental interest at stake, some consideration of the efficacy of the search being implemented -- that is, some measure of fit between the search and the desired objective -- is also relevant to the reasonableness analysis. *See, e.g.*, *Knights*, 534 U.S. at 119 (noting that the reasonableness of a search "is determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which [the search] is needed for the promotion of legitimate governmental interests." (internal quotation marks omitted)); *see also Board of Educ. v. Earls*, 536 U.S. 822, 834 (2002) ("Finally, this Court must consider the nature and immediacy of the government's concerns and the efficacy of the Policy in meeting them."). Here, NSA's acquisition of transactions through upstream collection is an essential and irreplaceable means of acquiring valuable foreign intelligence information that promotes the paramount governmental interest of protecting the Nation and conducting its foreign affairs. ~~(TS//SI//NF)~~

The AG and DNI have attested that a significant purpose of all acquisitions under Section 702, which includes those conducted by NSA's upstream collection, is to obtain foreign intelligence information. These acquisitions are conducted in accordance with FISC-approved targeting procedures reasonably designed to ensure that the acquisitions are directed "toward communications that are likely to yield the foreign intelligence information sought, and thereby

50 U.S.C. § 1801(e). (U)

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

afford a degree of particularity that is reasonable under the Fourth Amendment." [redacted] Mem. Op. at 39-40 (footnote omitted). Indeed, certain of the valuable foreign intelligence information NSA seeks to acquire through upstream collection of transactions simply cannot be acquired by any other means. (TS//SI//NF)

Specifically, as this Court has recognized, NSA's upstream collection "is particularly important because it is *uniquely capable* of acquiring certain types of targeted communications containing valuable foreign intelligence information," such as [redacted] Such foreign intelligence information is particularly useful, for example, [redacted][16] In

[16] More specifically, during the course of the Court's consideration of DNI/AG 702(g) Certification [redacted] the Government explained the unique value of NSA's [redacted]

[redacted]

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

addition, NSA's upstream collection enables NSA to acquire foreign intelligence information from [redacted] All of these types of communications are intercepted in transactions acquired through NSA's upstream collection. Valuable foreign intelligence information such as this simply cannot be obtained by means other than the acquisition of transactions through NSA's upstream collection. ~~(TS//SI//NF)~~

3. The Acquisition of Foreign Intelligence Information Contained in Transactions is Conducted Using the Least Intrusive Means Available. ~~(TS//SI//NF)~~

The fact that NSA's upstream collection acquires transactions that may contain several discrete communications, only one of which is to, from, or about a tasked selector, does not render NSA's upstream collection unreasonable. *See In re Directives*, 551 F.3d at 1015 ("It is settled beyond peradventure that incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful.") (citations omitted)); *see also United States v. Bin Laden*, 126 F. Supp. 2d 264, 280 (S.D.N.Y. 2000) ("[I]ncidental interception of a person's conversations during an otherwise lawful [Title III] surveillance is not violative of the Fourth Amendment."); *cf. Scott v. United States*, 436 U.S. 128, 140 (1978) (recognizing that "there are surely cases, such as the one at bar [involving a Title III wiretap], where the percentage of nonpertinent calls is relatively high and yet their interception was still reasonable"). Indeed, the Supreme Court has repeatedly rejected suggestions that reasonableness requires "the least intrusive search practicable." *City of Ontario v. Quon*, 130 S. Ct. 2619, 2632 (2010) (quotation marks omitted); *see, e.g., Earls*, 536 U.S. at 837 ("[T]his Court has repeatedly stated that reasonableness under the Fourth Amendment does not require employing the least intrusive means, because the logic of such elaborate less-restrictive-alternative arguments could raise insuperable barriers to the exercise of virtually all search-and-seizure powers." (internal quotation marks omitted)); *Vernonia*, 515 U.S. at 663 ("We have repeatedly refused to declare

[redacted]

~~(TS//SI//OC,NF)~~

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment."). ~~(TS//SI//NF)~~

Although not demanded by the Fourth Amendment, NSA is nevertheless conducting "the least intrusive search practicable" when it acquires a single transaction which may contain several discrete communications, only one of which may contain foreign intelligence information because it is to, from, or about a tasked selector. [redacted] Accordingly, at the time of acquisition, NSA generally cannot know whether a transaction contains only a single communication to, from, or about a tasked selector, or whether that transaction contains that single communication along with several other communications.[17] [redacted] also render the information technologically infeasible for NSA's upstream collection systems to extract only the discrete communication that is to, from, or about a tasked selector. The only way to obtain the foreign intelligence information contained within that discrete communication, therefore, is to acquire the entire transaction in which it is contained. The fact that other, non-pertinent information within the transaction may also be incidentally and unavoidably acquired simply cannot render the acquisition of the transaction unreasonable. *See United States v. Wuagneux*, 683 F.2d 1343, 1352-53 (11th Cir. 1982) (observing that "a search may be as extensive as reasonably required to locate the items described in the warrant," and on that basis concluding that it was "reasonable for the agents [executing the search] to remove intact files, books and folders when a particular document within the file was identified as falling within the scope of the warrant"); *United States v. Beusch*, 596 F.2d 871, 876-77 (9th Cir. 1979) (rejecting argument that "pages in a single volume of written material must be separated by searchers so that only those pages which actually contain the evidence sought may be seized"). ~~(TS//SI//NF)~~

At the same time, NSA is making every reasonable effort to ensure that its upstream collection acquires this singularly valuable foreign intelligence information in a manner that minimizes the intrusion into the personal privacy of United States persons to the greatest extent possible. As discussed above, these acquisitions are conducted in accordance with FISC-approved targeting procedures reasonably designed to ensure that the acquisitions are directed only "toward communications that are likely to yield the foreign intelligence information sought." [redacted] Mem. Op. at 39-40 (footnote omitted). The application of the targeting procedures further ensures that "[t]he targeting of communications pursuant to Section 702 is designed in a manner that diminishes the likelihood that United States person information will be obtained." [redacted] Mem. Op. at 23; *cf. In re Directives*, Docket No. 105B(g):07-01, Mem. Op. at 87 (USFISC April 25, 2008) (recognizing that "the vast majority of persons who are located overseas are non United States persons and that most of their communications are with other, non-United States persons, who are located overseas") (footnote omitted), *aff'd*, 551 F.3d 1004 (Foreign Int. Surv. Ct. Rev. 2008). Lastly, to the extent that United States person information is incidentally acquired in the acquisition of a whole transaction by NSA's upstream collection,

[17] *See* Government's response to questions 2(c) and (d) *infra*. (U)

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

such information will be handled in accordance with strict minimization procedures, as discussed in more detail below. ~~(TS//SI//NF)~~

4. United States Person Information Acquired Incidentally Through NSA's Acquisition of Transactions Containing Multiple Discrete Communications is Protected by NSA's Section 702 Minimization Procedures. ~~(TS//SI//NF)~~

As discussed above, the fact that NSA's upstream collection may result in the incidental acquisition of communications of United States persons cannot, by itself, render the overall collection unreasonable. Instead, courts have repeatedly found support for the constitutionality of foreign intelligence activities resulting in the incidental acquisition of United States person information in the existence and application of robust minimization procedures. *See, e.g., In re Directives*, 551 F.3d at 1015 (recognizing that minimization procedures are a "means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons"); [redacted] Mem. Op. at 40 (concluding that minimization procedures meeting the definition in 50 U.S.C. § 1801(h)(1) "constitute a safeguard against improper use of information about United States persons that is inadvertently or incidentally acquired, and therefore contribute to the Court's overall assessment that the targeting and minimization procedures are consistent with the Fourth Amendment"). As explained below, NSA's current Section 702 minimization procedures, which this Court previously has found to satisfy the definition of minimization procedures in 50 U.S.C. § 1801(h)(1),[18] adequately protect the privacy interests of United States persons whose communications may be incidentally acquired through NSA's upstream collection and thus contribute significantly to the overall reasonableness of that collection. ~~(TS//SI//NF)~~

At the outset, it is worth noting that NSA's acquisition of Internet transactions containing multiple discrete communications does not necessarily increase the risk that NSA will incidentally acquire United States person information. For example, as discussed above, the [redacted] means by which NSA ensures it does not intentionally acquire wholly domestic communications limits the acquisition of certain transactions such as [redacted] to persons located outside the United States, who reasonably can be presumed to be non-United States persons. Thus, to the extent that the [redacted] of those non-United States persons contain communications that are not to, from, or about a targeted selector, those communications are unlikely to be United States person communications. *See In re Directives*, Docket No. 105B(g):07-01, Mem. Op. at 87 (recognizing that "the vast majority of persons who are located overseas are non United States persons and that most of their communications are with other, non-United States persons, who are located overseas") (footnote omitted). For this same reason, the risk that United States person information would be obtained through the acquisition of a [redacted] is no greater than in the acquisition of a [redacted]

[18] 50 U.S.C. § 1801(h)(1) defines "minimization procedures" as "specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." (U)

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

[redacted] ~~(TS//SI//NF)~~

a. Acquisition (U)

As discussed above, with limited exceptions,[19] it is technologically infeasible for NSA's upstream collection to acquire only the discrete communication to, from, or about a tasked selector that may be contained in a transaction containing multiple discrete communications. That does not mean, however, that the minimization procedures governing NSA's upstream collection do not adequately minimize the acquisition of any United States person information that may be contained in those transactions. Specifically, minimization procedures must be reasonably designed to minimize the acquisition of nonpublicly available information concerning unconsenting United States persons "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. § 1801(h)(1). As discussed above, the *only* way to obtain the foreign intelligence information contained within a discrete communication is to acquire the entire transaction in which it is contained. Thus, to the extent that United States person information may be contained within other discrete communications not to, from, or about the target in that transaction, the acquisition of such United States person information would be "consistent with the need of the United States to obtain . . . foreign intelligence information." ~~(TS//SI//NF)~~

Congress has recognized that "in many cases it may not be possible for technical reasons to avoid acquiring all information" when conducting foreign intelligence surveillance. H.R. Rep. No. 95-1283, pt. 1, at 55 (1978); *see also id.* at 56 ("It may not be possible or reasonable to avoid acquiring all conversations."); *cf. Scott*, 436 U.S. at 140 (recognizing that Title III "does not forbid the interception of all nonrelevant conversations, but rather instructs the agents to conduct the surveillance in such as manner as to 'minimize' the interception of such conversations"). Rather, in situations where, as here, it is technologically infeasible to avoid incidentally acquiring communications that are not to, from, or about the target, "the reasonable design of the [minimization] procedures must emphasize the minimization of retention and dissemination." H.R. Rep. No. 95-1283, pt. 1, at 55. ~~(TS//SI//NF)~~

b. Retention (U)

In addition, for reasons discussed more fully below, nothing in the statutory definition of minimization procedures obligates NSA to immediately destroy any United States person information in a communication that is not to, from, or about a tasked selector within a transaction acquired by NSA's upstream collection. ~~(TS//SI//NF)~~

[19] *See supra* footnote 6. (U)

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

i. Destruction Is Not Technologically Feasible ~~(TS//SI//NF)~~

First, Congress intended that the obligation to destroy non-pertinent information would attach only if the destruction of such information is feasible. *See* H.R. Rep. No. 95-1283, pt. 1, at 56 ("By minimizing retention, the committee intends that information acquired, which is not necessary for obtaining[,] producing, or disseminating foreign intelligence information, be destroyed *where feasible*." (emphasis added)). That is because Congress recognized that in some cases, the pertinent and non-pertinent information may be co-mingled in such a way as to make it technologically infeasible to segregate the pertinent information from the non-pertinent information and then destroy the latter. *See id.* ("The committee recognizes that it may not be feasible to cut and paste files or erase part of tapes where some information is relevant and some is not."). ~~(TS//SI//NF)~~

A transaction containing several communications, only one of which contains the tasked selector, is to NSA's systems technologically indistinguishable from a transaction containing a single message to, from, or about a tasked selector. That is true both for NSA's collection systems and for the NSA systems that process and then route Section 702-acquired information to NSA's corporate stores. Thus, unlike other instances where it is technologically possible for certain kinds of communications to be recognized, segregated, and prevented from being routed to NSA's corporate stores, the transaction as a whole, including all of the discrete communications that may be included within it, is forwarded to NSA corporate stores, where it is available to NSA analysts. ~~(TS//SI//NF)~~

The transaction is likewise not divisible into the discrete communications within it even once it resides in an NSA corporate store. That is because NSA assesses that it is not technologically feasible to extract, post-acquisition, only the discrete communication that is to, from, or about a tasked selector within a transaction without destabilizing -- and potentially rendering unusable -- some or all of the collected transaction, including the single, discrete communication which is to, from or about the tasked selector. Thus, an NSA analyst cannot, for example, simply cut out any pertinent part of the transaction (i.e., the discrete communication that contains the tasked selector), paste it into a new record, and then discard the remainder. In this way, the transactions at issue here are a present-day version of the very same problem that Congress recognized over thirty years earlier -- i.e., that in some cases, "it might not be feasible to cut and paste files . . . where some information is relevant and some is not." H.R. Rep No. 95-1283, pt.1, at 56. Given that Congress recognized it might be necessary to retain all acquired information regardless of its pertinence because destruction of the non-pertinent information may not be feasible, minimization procedures that permit the retention of transactions in their entireties because their further divisibility is infeasible (if not technologically impossible) are consistent with the statutory requirement that such procedures minimize the retention of United States person information. ~~(TS//SI//NF)~~

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

ii. Retention of United States Person Information Can Be Effectively Minimized Through Restrictions on its Retrieval ~~(TS//SI//NF)~~

Second, although it is not required that all non-pertinent United States person information be destroyed, NSA's retention of non-pertinent information concerning innocent United States persons is not without bounds. FISA's legislative history suggests that the retention of such information could still be effectively minimized through means other than destruction. *See* H.R. Rep. No. 95-1283, pt. 1, at 56 ("There are a number of means and techniques which the minimization procedures may require to achieve the purposes set out in the definition."). Of particular relevance here, Congress recognized that minimizing the retention of such information can be accomplished by making the information "not retrievable by the name of the innocent person" through the application of "rigorous and strict controls." *Id.* at 58-59. Those "rigorous and strict controls," however, need only be applied to the retention of United States person information "for purposes other than counterintelligence or counterterrorism." *Id.* That is because Congress intended that "a significant degree of latitude be given in counterintelligence and counterterrorism cases with respect to the retention of information." *Id.* at 59. ~~(TS//SI//NF)~~

NSA's current Section 702 minimization procedures flatly prohibit the use of United States person names or identifiers to retrieve any Section 702-acquired communications in NSA systems. *See, e.g.*, Amendment 1 to DNI/AG 702(g) Certification [redacted] Ex. B, filed [redacted] 2010, § 3(b)(5) (hereinafter "NSA Section 702 minimization procedures"). This "rigorous and strict control[]" applies even to United States person information that relates to counterintelligence or counterterrorism, despite Congress's stated intent that agencies should have "a significant degree of latitude . . . with respect to the retention of [such] information." H.R. Rep. No. 95-1283, pt. 1, at 59; *see id.* at 58-59 (recognizing that "for an extended period it may be necessary to have information concerning [the] acquaintances [of a hypothetical FISA target] retrievable" for analytic purposes, even though "[a]mong his contacts and acquaintances . . . there are likely to be a large number of innocent persons"). NSA's current Section 702 minimization procedures thus require the retention of information concerning United States persons (innocent or otherwise) to be minimized to a significantly greater degree than is necessary for those procedures to be reasonable. ~~(TS//SI//NF)~~

Of course, the Government seeks the Court's approval of revised NSA Section 702 minimization procedures that would enable NSA analysts to use United States person identifiers as selection terms if those selection terms are reasonably likely to return foreign intelligence information. E.g., DNI/AG 702(g) Certification [redacted] Ex. B, filed Apr. 20, 2011, § 3(b)(5). Under these revised NSA Section 702 minimization procedures, the use of such selection terms must be approved in accordance with NSA procedures. *Id.* The Government is still in the process of developing the NSA procedures governing the use of United States person identifiers as selection terms. Until those procedures are completed, NSA analysts will not begin using United States person identifiers as selection terms. The Government will ensure that these NSA procedures contain "rigorous and strict controls" on the retrieval of United States person information consistent with statutory requirements and Congressional intent. H.R. Rep. No. 95-1283, pt. 1, at 59. ~~(TS//SI//NF)~~

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

c. Dissemination (U)

As discussed above, the NSA current Section 702 minimization procedures prohibit the use of United States person identifiers to retrieve any Section 702-acquired communications in NSA systems. Accordingly, the only way incidentally acquired United States person information currently will be reviewed by an NSA analyst is if that information appears in a communication that the analyst has retrieved using a permissible query term -- i.e., one that is reasonably likely to return information about non-United States person foreign intelligence targets. *See* NSA Section 702 minimization procedures, § 3(b)(5). Any identifiable United States person information contained in a communication retrieved in this manner would be subject to the dissemination restrictions in the NSA Section 702 minimization procedures, which operate to ensure that any dissemination of United States person information is consistent with the Act. These restrictions apply regardless of whether the United States person information is contained in a discrete communication that is to, from, or about a tasked selector. Moreover, the same dissemination restrictions will continue to apply to any United States person information retrieved through the use of a United States person identifier as a selection term in accordance with NSA's revised 702 minimization procedures. Indeed, given the small probability that an incidentally acquired communication of a United States person that is not to, from, or about a tasked selector would contain foreign intelligence information or evidence of a crime, it is highly unlikely that NSA would disseminate any information from that incidentally acquired communication, let alone information concerning the United States person. ~~(TS//SI//NF)~~

[redacted]

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

[redacted]

20 [redacted] ~~(TS//SI//NF)~~

21 [redacted] ~~(TS//SI//NF)~~

[22] *See* footnote 22 below. (S)

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[redacted]

[redacted]

[redacted]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

[redacted]

c. **The May 2 Letter states that NSA is not presently capable of "separating out individual pieces of information" contained within [redacted] May 2 Letter at 3. Please explain why and state whether it would be feasible for NSA to implement such capability, either at the time of acquisition or thereafter.** ~~(TS//SI//NF)~~

d. **Can [redacted] be identified as distinct from other, discrete communications between users, either at the time of acquisition or thereafter? If so, can NSA filter its Section 702 collection on this basis?** ~~(TS//SI//NF)~~

[redacted]

Except as described above, at the time of acquisition, NSA is not presently capable of separating out transactions that contain multiple electronic communications into logical constituent parts without destabilizing -- and potentially rendering unusable -- some or all of the entire collected transaction, including any particular communication therein which is in-fact to, from, or about the tasked selector. Each electronic communication service provider develops protocols that perform the services being provided in a manner designed to be economical in speed, size, and other factors that the provider considers important. [redacted]

[25] An NSA analyst would, however, be able to copy a portion of the rendered view of a transaction contained in a NSA corporate store and then paste it into a new record on a different system, such as an analytic store. Even so, the original transaction from which that copy was made would be retained in the corporate store in its original state, which cannot be altered for the reasons discussed below. ~~(TS//SI//NF)~~

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

Each of the major providers change protocols often to suit their own business purposes, and it is therefore generally not possible for NSA to isolate or separate out individual pieces of information contained within single transactions at the time of NSA acquisition. Any protocol in use today could easily be changed by the provider tomorrow [redacted] ~~In short, except in cases involving~~ [redacted] described above, at the time of acquisition it is not technologically feasible for NSA to extract any particular communication that is to, from, or about a tasked selector within a transaction containing multiple discrete communications. ~~(TS//SI//NF)~~

For the same reasons that protocol volatility and myriad user settings prevent the extraction of only discrete communications at the point of acquisition, it is not technologically feasible to extract, post-acquisition, only the specific communication(s) to, from, or about a tasked selector within a transaction without destabilizing -- and potentially rendering unusable -- some or all of the collected transaction, including any particular communication therein which is to, from, or about the tasked selector. Thus, an NSA analyst cannot, for example, simply cut out the discrete communication that contains the tasked selector, paste it into a new record, and then discard the remainder. ~~(TS//SI//NF)~~

3. The May 2 Letter notes that NSA uses Internet Protocol (IP) filtering and [redacted] to prevent the intentional acquisition of communications as to which the sender and all known recipients are inside the United States. May 2 Letter at 3. ~~(TS//SI//NF)~~

a. Please describe how NSA applies IP filtering in the context of [redacted] ~~(TS//SI//NF)~~

i. [redacted] ~~(TS//SI//NF)~~

ii. [redacted] ~~(TS//SI//NF)~~

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

NSA acquires Internet communications by collecting the individual packets of data that make up those communications. As required by NSA's targeting procedures, all Internet communications data packets that may contain abouts information that NSA intercepts through its Section 702 upstream collection must either pass through an "Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas," or

[redacted]

~~(TS//SI//OC,NF)~~

[redacted]

~~(TS//SI//OC,NF)~~

[redacted]

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

[redacted] Accordingly, NSA cannot prevent the acquisition of, or even mark for separate treatment, those types of transactions that may feature multiple discrete communications ([redacted] ~~(TS//SI//OC,NF)~~

b. **In the collection of "to/from" communications, are the communicants always the individual users of particular facilities [redacted], or does NSA sometimes consider [redacted] Please explain.** ~~(TS//SI//NF)~~

In the collection of "to/from" communications, NSA considers the communicants as being the individual users of particular selectors. More particularly, NSA considers those individual users to be the senders and intended recipients of "to/from" communications. Conversely, NSA does not consider [redacted] ~~(TS//SI//NF)~~

4. **How, in terms of numbers and volume, does NSA's collection of [redacted] under Section 702 compare with the collection of discrete Internet communications (such as e-mail messages) between or among individual users?** ~~(TS//SI//NF)~~

As a result of the present technological limitations [redacted] NSA cannot precisely measure the number of transactions that might contain information or data representing several discrete communications [redacted] for purposes of comparing that figure with transactions containing a single, discrete communication [redacted] without manually examining each transaction that NSA has acquired. However, in an attempt to provide an estimate of the volume of such collection at the Court's request, NSA performed a series of queries into the SIGINT Collection Source System of Record that holds the relevant transactions in question. [redacted] Results were sampled manually to confirm collection of [redacted] Results were reviewed for three randomly selected days in April, averaged to produce an estimated figure of collection of [redacted] for the month of April. This figure was then compared to the total take of Section 702 upstream collection of web activity for the month. From this sample, NSA estimates that approximately 9% of the monthly Section 702 upstream collection of [redacted][26] It is important

[26] NSA notes that it is likely that this 9% figure includes [redacted] of the user of the targeted selector him/herself. ~~(TS//SI//NF)~~

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

to note that this was a manually intensive and imprecise means to quantify the volume of [redacted] collection and should not be interpreted to suggest that any technological method of pre-filtering can be applied to the collection before it is available to the analyst. ~~(TS//SI//NF)~~

5. Given that some of the information acquired through upstream collection is likely to constitute "electronic surveillance" as defined in 50 U.S.C. § 1801(f)(2) that has not been approved by this Court, how does the continued acquisition of, or the further use or dissemination of, such information comport with the restrictions of 50 U.S.C. § 1809(a)(1) and (a)(2)? ~~(TS//SI//NF)~~

I. THE CONTINUED ACQUISITION, USE, AND DISSEMINATION OF INFORMATION ACQUIRED THROUGH UPSTREAM COLLECTION DOES NOT VIOLATE 50 U.S.C. § 1809. ~~(TS//SI//NF)~~

A. Introduction (U)

Section 702 of FISA, as codified at 50 U.S.C. § 1881a, provides that "[n]otwithstanding any other provision of law," upon the issuance of an appropriate Order from the Court, the Attorney General (AG) and the Director of National Intelligence (DNI) may jointly authorize the targeting of non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information as long as certain conditions set out in subsection 702(b) are met. The joint authorizations of the AG and the DNI authorized NSA's upstream acquisition of communications that are to, from, or about a tasked selector. The Court, in turn, approved the implementing certifications as well as the use of proffered targeting and minimization procedures. Accordingly, because the acquisition of communications to, from, or about a tasked selector was authorized by the AG and DNI, and the Court approved the certifications and procedures used to implement those authorizations, NSA's acquisition of such communications upstream does not constitute unauthorized electronic surveillance and, therefore, does not violate the terms of 50 U.S.C. § 1809. ~~(TS//SI//NF)~~

As noted above, the Government readily acknowledges that it did not fully describe to the Court that the upstream collection technique would result in NSA acquiring [redacted] types of Internet transactions that could include multiple individual, discrete communications [redacted] As discussed below, however, this omission does not invalidate the AG and DNI's prior authorizations. Nor does it mean that the incidental acquisition of communications that are not to, from, or about a tasked selector as a consequence of obtaining communications that are to or from a tasked selector or contain reference to a tasked selector, exceeds the scope of those authorizations. For the same reasons, the Government respectfully suggests that the Orders of

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

this Court upon which those authorizations rely likewise remain valid. Thus, Section 1809 is not implicated by NSA's upstream collection activities under Section 702. ~~(TS//SI//NF)~~

B. Statutory Framework (U)

i. Section 1809 (U)

Under Subsection 1809(a), a person is guilty of a criminal offense if he or she "intentionally (1) engages in electronic surveillance under color of law, except as authorized by this Act . . . ; or (2) disclose[s] or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by this Act."[27] (U)

For purposes of Section 1809 the issue is whether the Government's prior failure to fully explain to the Court the steps NSA must take in order acquire communications to, from, or about a tasked selector, and certain technical limitations regarding the IP address filtering it applies, means that the acquisition of such communications was not authorized by the DNI and AG, and inconsistent with Court approval of the targeting and minimization procedures. ~~(TS//SI//NF)~~

ii. Section 702 Collection Authorizations ~~(S)~~

Pursuant to 50 U.S.C. § 1881a(a), "notwithstanding any other provision of law," the AG and the DNI may jointly authorize for a period of up to one year the targeting of non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information, subject to targeting and minimization procedures approved by this Court, and certain limitations set out in §1881a(b). Authorizations are premised on certifications to the Court, in which the AG and DNI attest to the fact that, among other things, the targeting and minimization procedures comply with certain statutory requirements and the Fourth

[27] This Court has previously noted that the legislative history of this provision focuses on a predecessor bill that was substantially different from the provision subsequently enacted and codified. *See* [redacted] Mem. Op. at 6-7 (Dec. 10, 2010). Yet, both the predecessor bill and the codified provision use the word intentionally, which has been described as "carefully chosen" and intended to limit criminal culpability to those who act with a "conscious objective or desire" to commit a violation. *See* H.R. Rep. No. 95-1283, pt.1, at 97 (1978) ("The word 'intentionally' was carefully chosen. It is intended to reflect the most strict standard for criminal culpability. . . . The Government would have to prove beyond a reasonable doubt both that the conduct engaged in was in fact a violation, and that it was engaged in with a conscious objective or desire to commit a violation."). Based upon discussions between responsible NSA officials and the Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) and DOJ and ODNI's review of documents related to this matter, DOJ and ODNI have not found any indication that there was a conscious objective or desire to violate the authorizations here. ~~(TS//SI//NF)~~

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

Amendment. 50 U.S.C. § 1881a(g)(2). Authorizations become effective "upon the issuance of an order [of this Court]" approving the certification and the use of the targeting and minimization procedures as consistent with the statute and the Fourth Amendment. *Id.* §§ 1881a(a) (AG and DNI authorizations go into effect upon "issuance of an order"); 1881a(i)(2)-(3) (laying out scope of FISC review).[28] ~~(TS//SI//NF)~~

Thus, if an acquisition is authorized by the AG and DNI, and the certification and targeting and minimization procedures which implement that authorization are approved by the Court, and the authorization remains valid, then the acquisition does not constitute unauthorized electronic surveillance under 50 U.S.C. § 1801(f)(2) and is not a violation of 50 U.S.C. § 1809. ~~(TS//SI//NF)~~

C. At a Minimum, the Upstream Acquisition of Single, Discrete Communications To, From, or About a Tasked Selector Was Authorized by the AG and the DNI ~~(TS//SI//NF)~~

The relevant AG and DNI authorizations and the targeting procedures the AG approved explicitly permit the acquisition of Internet communications that are to, from, or about a tasked selector. *See, e.g.*, NSA Targeting Procedures at 1 (describing the safeguards used in the acquisition of "about" as compared with "to/from" communications). In addition, the accompanying Affidavits of the Director of NSA described upstream collection in a paragraph detailing the various methods of obtaining such acquisitions. *See, e.g.*, DNI/AG 702(g) Certification [redacted] Affidavit of General Keith B. Alexander, Director, NSA, filed July 16, 2010, ¶ 4. Thus, it is clear that the authorizations permit – at a minimum – the upstream acquisition of single, discrete communications to, from, or about a tasked selector. ~~(TS//SI//NF)~~

As described in detail in response to questions 2 and 3 above, due to certain technological limitations, in general the only way NSA can currently acquire as part of its upstream collection single, discrete communications to, from, or about a tasked selector [redacted] is by obtaining the Internet transactions of which those communications are a part. An Internet transaction can include either a single, discrete communication to, from, or about a tasked

[28] For reauthorizations, the AG and the DNI submit, to the extent possible, a certification to the FISC laying out, among other things, the targeting and minimization procedures adopted at least 30 days prior to the expiration of the prior authorization. The prior authorization remains in effect, notwithstanding the otherwise applicable expiration date, pending the FISC's issuance of an order with respect to the certification for reauthorization. 50 U.S.C. § 1881a(i)(5). The scope of the court's review is the same for reauthorizations as it is for initial authorizations. *Id.* § 1881a(i)(5)(B). (U)

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

selector [redacted], or several discrete communications, only one of which may be to, from, or about a tasked selector[redacted] ~~(TS//SI//NF)~~

Where an Internet transaction includes multiple communications, not all of which are to, from, or about a tasked selector, it currently may not be technologically feasible for NSA to separate out, at the time of acquisition or thereafter, the discrete electronic communications within that transaction that are to, from, or about a tasked selector. Indeed, at the time of acquisition, NSA's upstream Internet collection devices are, with limited exception, not capable of distinguishing or further separating discrete electronic communications [redacted] within a single Internet transaction. Thus, in some cases, NSA can collect communications to, from, or about a tasked selector, as authorized by the certification, only by obtaining the Internet transaction of which those communications may be just a part. ~~(TS//SI//NF)~~

In this respect, the upstream acquisition of Internet transactions which contain multiple, discrete communications not all of which are (and, in some instances, only one of which is) to, from or about a tasked selector is akin to the Government's seizure of a book or intact file that contains a single page or document that a search warrant authorizes the government to seize. In *United States v. Wuagneux*, 683 F.2d 1343, for example, the Eleventh Circuit rejected appellants' argument that a search was unreasonable because the agents seized an entire file, book, or binder if they identified a single document within the file, book, or binder as being within the authorization of the warrant. As the court explained, "a search may be as extensive as reasonably required to locate items described in the warrant." *Id.* at 1352. It was therefore "reasonable for the agents to remove intact files, books and folders when a particular document within the file was identified as falling within the scope of the warrant." *Id.* at 1353. *See also United States v. Rogers*, 521 F.3d 5, 10 (1st Cir. 2008) (concluding that a videotape is a "plausible repository of a photo" and that therefore a warrant authorizing seizure of "photos" allowed the seizure and review of two videotapes); *United States v. Christine*, 687 F. 2d 749, 760 (3d Cir. 1982) (*en banc*) (emphasizing that "no tenet of the Fourth Amendment prohibits a search merely because it cannot be performed with surgical precision. Nor does the Fourth Amendment prohibit seizure of an item, such as a single ledger, merely because it happens to contain other information not covered by the scope of the warrant."); *United States v. Beusch*, 596 F.2d 871, 876-77 (9th Cir. 1979) (rejecting argument that "pages in a single volume of written material must be separated by searchers so that only those pages which actually contain the evidence may be seized"). ~~(TS//SI//NF)~~

That the certifications by the AG and DNI did not specifically describe this aspect of NSA's upstream collection does not mean that collection was unauthorized by the AG and DNI. Again, case law involving the reasonableness of searches conducted pursuant to criminal search warrants is instructive on this point. For example, in *Dalia v. United States*, 441 U.S. 238, 259 (1979), the Supreme Court recognized that "[o]ften in executing a warrant the police may find it

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

necessary to interfere with privacy rights not explicitly considered by the judge who issued the warrant." *Id.* at 257. *See United States v. Grubbs*, 547 U.S. 90, 98 (2006) ("'Nothing in the language of the Constitution or in this Court's decisions interpreting that language suggests that, in addition to the [requirements set forth in the text], search warrants also must include a specification of the precise manner in which they are to be executed.'") (quoting *Dalia*, 441 U.S. 238, 257 (1979)). This is especially true where, as in *Dalia*, "[t]here is no indication that [the] intrusion went beyond what was necessary" to effectuate the search authorized. *Dalia*, 441 U.S. at 258 n. 20. ~~(TS//SI//NF)~~

Like the seizure of an entire book or file simply because it contained a single page or document within the scope of the warrant, NSA only acquires an Internet transaction containing several discrete communications if at least one of those communications within the transaction is to, from, or about a tasked selector. Moreover, unlike the agents in *Wuagneux*, who presumably could have opted to seize only the responsive pages out of the books and files searched, except in limited circumstances, NSA has no choice but to acquire the whole Internet transaction in order to acquire the to, from, or about communication the DNI and AG authorized NSA to collect. NSA only acquires an Internet transaction if *in fact* it contains at least one communication to, from, or about a tasked selector. NSA's acquisition of Internet transactions containing several discrete communications, only one of which is to, from, or about a tasked selector, is therefore "as extensive as reasonably required to locate the items described" in the DNI and AG's authorization, and thus cannot be said to exceed the scope of that authorization. ~~(TS//SI//NF)~~

Moreover, as described in response to questions 1(b)(ii) and (iii), the Government has concluded that such collection fully complies with the statutory requirements and the Fourth Amendment. Having now considered the additional information that is being presented to this Court, the AG and DNI have confirmed that their prior authorizations remain valid. Accordingly, Government personnel who rely on those authorizations to engage in ongoing acquisition are not engaging in unauthorized electronic surveillance, much less doing so "intentionally." ~~(TS//SI//NF)~~

D. The Court Approved the Certifications and Targeting and Minimization Procedures Used to Implement the Authorizations of the AG and DNI ~~(TS//SI//NF)~~

A second issue concerns whether this Court's orders cover the full scope of the authorizations, and, if not, whether that affects the validity of the AG and DNI authorizations. Like the AG and DNI authorizations, in approving the applicable certifications and the use of the proffered targeting and minimization procedures this Court's Opinions and Orders clearly contemplated and approved some upstream collection of communications to, from, or about a target. *See, e.g.,* [redacted] Mem. Op. at 15-17 (describing acquisition of communications to, from,

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

and about a target).[29] Thus, for the reasons described above, the acquisition of Internet transactions that include at least one communication to, from, or about a target falls within the scope of the Court's Orders – even if additional communications are also incidentally acquired due to limits in technology. ~~(TS//SI//NF)~~

The fact that the Government did not fully explain to the Court all of the means by which such communications are acquired through NSA's upstream collection techniques does not mean that such acquisitions are beyond the scope of the Court's approval, just as in the criminal context a search does not exceed the scope of a warrant because the Government did not explain to the issuing court all of the possible means of execution, even when they are known beforehand and could possibly implicate privacy rights. *See Dalia*, 441 U.S. at 257 n.19 (noting that "[n]othing in the decisions of this Court . . . indicates that officers requesting a warrant should be constitutionally required to set forth the anticipated means for execution even in those cases where they know beforehand that [an additional intrusion such as] unannounced or forced entry likely will be necessary."). In addition, as discussed herein, the incidental acquisitions do not go beyond what is reasonably necessary to acquire the foreign intelligence information contained in a communication to, from, or about a targeted selector within a transaction. *See id.* at 258 n. 20. ~~(TS//SI//NF)~~

In any event, the Government believes that the additional information should not alter the Court's ultimate conclusion that the targeting and minimization procedures previously approved are consistent with the statutory requirements, including all the requirements of § 1881a(b), and the Fourth Amendment, and the Court's orders therefore remain valid. *Cf. Franks v. Delaware*, 438 U.S. 154 (1978) (establishing that a search warrant is valid unless it was obtained as the result of a knowing and intentional false statement or reckless disregard for the truth and the remaining content is insufficient to establish the requisite probable cause needed to obtain the warrant). ~~(TS//SI//NF)~~

Pursuant to § 1881a, the Court reviews the following issues: (i) whether the AG and DNI certifications contain all the required elements; (ii) whether the targeting procedures are consistent with the requirements of § 1881a(d)(1); (iii) whether the minimization procedures are consistent with § 1881a(i)(e)(1); and (iv) whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment. 50 U.S.C. § 1881a(i)(2), (3). *See also id.* § 1881a(i)(5)(B) (specifying that reauthorizations are to be reviewed under the same

[29] Each of the relevant 2010 FISC Orders is based on the "reasons stated in the Memorandum Opinion issued contemporaneously herewith." These Opinions, in turn, rely on the analysis conducted by the Court in Dockets [redacted], which incorporate and rely on the analysis of earlier FISC Opinions, including Docket 702(i)-08-01. ~~(TS//SI//NF)~~

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

standards). The Government believes that the Court's ultimate conclusions with respect to each of these issues should not change based on the additional information provided. ~~(TS//SI//NF)~~

First, there is no suggestion that the prior certifications failed to contain all the required elements. ~~(TS//SI//NF)~~

Second, while the Government acknowledges that it did not fully explain to the Court the steps NSA must take in order to implement its Section 702 upstream Internet collection techniques, and certain technical limitations regarding its IP address filtering, the Court did approve the DNI/AG certifications and the use of targeting and minimization procedures which authorized the acquisition of communications to, from, or about tasked selectors. As discussed above and in response to questions 1(b)(ii) (iii) and 3, Internet transactions are collected because they contain at least one discrete communication to, from, or about a tasked selector. Each tasked selector has undergone review, prior to tasking, designed to ensure that the user is a non-United States person reasonably believe to be located outside the United States. Moreover, with respect to "abouts" communications, for the reasons discussed in the response to question 1(b)(ii), NSA's targeting procedures are reasonably designed to prevent the intentional acquisition of any communications as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States.[30] Thus, NSA is targeting persons reasonably believed to be outside the United States and is not intentionally acquiring communications in which both the sender and all intended recipients are known at the time of acquisition to be in the United States. ~~(TS//SI//NF)~~

Third, as described throughout, in many cases, it is not technologically feasible for NSA to acquire only Internet transactions that contain a single, discrete communication to, from, or about a tasked selector that may be contained in an Internet communication containing multiple discrete [redacted] communications. As discussed in detail in response to questions 1(b)(ii) and (iii), this does not mean that NSA's procedures do not adequately minimize the acquisition of any U.S. person information that may be contained within those transmissions. Rather, the minimization procedures fully comport with all statutory requirements. ~~(TS//SI//NF)~~

[30] As the Court is aware, § 1881a(b)(4) provides that an acquisition authorized under section 702, "may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States . . ." Although this prohibition could be read at first glance to be absolute, another provision of Section 702 indicates otherwise. Specifically, § 1881a(d)(1)(B) provides that the targeting procedures that the AG, in consultation with the DNI, must adopt in connection with an acquisition authorized under section 702 need only be "reasonably designed to . . . prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." (U)

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

Finally, as described in response to question 1(b)(iii), the targeting and minimization procedures fully comply with the Fourth Amendment. ~~(TS//SI//NF)~~

Thus, the additional information the Government has provided concerning details of its upstream collection does not – in the Government's view – undercut the validity of the targeting or minimization procedures. ~~(TS//SI//NF)~~

E. Compliance with the Authorizations: Use and Disclosure ~~(TS//SI//NF)~~

As described above, § 1809(a)(2) criminalizes the intentional use and disclosure of electronic surveillance, "knowing or having reason to know that the information was obtained through electronic surveillance not authorized by this Act." Having concluded that the upstream collection conducted by NSA falls within the scope of the relevant authorizations, the Government respectfully submits that the continued use and disclosure of such information is likewise valid, so long as the minimization procedures approved by the Court (and discussed in detail in response to questions 1(b)(ii) and (iii)) are followed.[31] ~~(TS//SI//NF)~~

6. Please provide an update regarding the [redacted] over collection incidents described in the government's letter to the Court dated April 19, 2011.

The April 19, 2011, notice to the Court described two overcollection incidents involving entirely unrelated communications that had been [redacted] The notice also advised that as part of its continued investigation into these incidents, NSA would examine other systems to determine whether similar [redacted] issues occurred in those systems. ~~(TS//SI//NF)~~

The first incident described in the April 19 notice involved [redacted] Each [redacted] contained at least one communication to, from, or about a Section 702-tasked selector, but also [redacted] unrelated communications. This overcollection started [redacted]

[31] Although this analysis has focused on acquisitions conducted pursuant to the 2010 Section 1881a Authorizations, the Government believes that, for all of the reasons discussed herein, the upstream collection conducted pursuant to previous certifications authorized under Section 1881a of the Foreign Intelligence Surveillance Act of 1978, as amended, the Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (Aug. 5, 2007), [redacted] falls within the scope of the relevant authorizations and Orders of this Court. ~~(TS//SI//NF)~~

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

[redacted] ~~(TS//SI//NF)~~

[redacted] All such communications will be processed in accordance with NSA's minimization procedures.[32] The Government will advise the Court of the final disposition of these communications. [redacted] ~~(TS//SI//NF)~~

The second-described [redacted] incident involved overcollection [redacted]. As described in the April 19 notice, on March 28, 2011, NSA discovered a [redacted] of Section 702-acquired communications that had not been properly [redacted] In contrast to the communications overcollected between [redacted] discussed above, the [redacted] acquired as a result of the [redacted] overcollection incident involved fewer communications [redacted]

[32] In particular, section 3(b)(1) of NSA's Section 702 Minimization Procedures state:

> Personnel will exercise reasonable judgment in determining whether information acquired must be minimized and will destroy inadvertently acquired communications of or concerning a United States person at the earliest practicable point in the processing cycle at which such communication can be identified either: as clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information); or, as not containing evidence of a crime which may be disseminated under these procedures. Such inadvertently acquired communications of or concerning a United States person may be retained no longer than five years in any event. **The communications that may be retained include electronic communications acquired because of limitations on NSA's ability to filter communications.**

(Emphasis added). ~~(S//SI)~~

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

As in the [redacted] incident, each [redacted] contains at least one communication that is to, from, or about a Section 702-tasked selector. ~~(TS//SI//NF)~~

As of April 11, 2011, NSA began to sequester in its Collection Stores all communications involving the affected [redacted]. NSA was deliberately overinclusive in adding objects to the [redacted]; while some of these objects include [redacted] other objects consist of only one communication to, from, or about a Section 702-tasked selector. ~~(TS//SI//NF)~~

Since the filing of the April 19 notice, NSA has continued to evaluate collection from [redacted] and has observed no evidence of [redacted] issues other than the above-described issues [redacted] ~~(TS//SI//NF)~~

NSA has identified no reporting based upon overcollected communications and is currently exploring options to automate ways to accelerate identification of [redacted] NSA anticipates that it will be able to reach a decision by June 30, 2011, on whether this approach is effective. ~~(TS//SI//NF)~~

[redacted] ~~(TS//SI//NF)~~

The April 19 notice also advised the Court that NSA would "examine [redacted] and other upstream collection systems to ensure that similar [redacted] problems are not occurring in those systems." NSA now reports that unlike the most recent [redacted]

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

these other systems were designed [redacted][33] [redacted] ~~(TS//SI//NF)~~

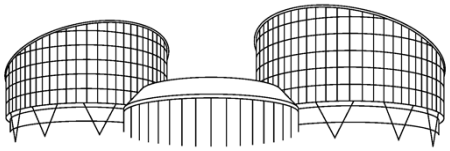
7. **Are there any other issues of additional information that should be brought to the Court's attention while it is considering the certifications and amendments filed in the above-captioned dockets?**

At this time, the Department of Justice (DOJ) and Office of the Director of National Intelligence (ODNI) are currently investigating certain possible incidents of non-compliance about which the Department of Justice intends to file preliminary notices in accordance with the rule of this Court. These incidents do not relate to any of the matters discussed in this filing and, based on the information currently available to DOJ and ODNI, the Government does not believe that the nature of these incidents is sufficiently serious such that they would bear on the Court's consideration of the certifications and amendments filed in the above-captioned dockets. ~~(S//OC,NF)~~

[33] As discussed in response to question 2(c) and (d), NSA has the ability to separate out individual pieces of information in certain cases [redacted] In the course of the investigation into the most recent [redacted] incident, NSA additionally identified [redacted] Though testing demonstrated the possibility that incompletely processed communications could have been forwarded through the SIGINT system, NSA has identified no actual overcollection that occurred as a result. NSA is currently in the process of developing a software fix designed to properly process such communications under the limited circumstances in which overcollections could occur. Until such a fix can be tested and deployed, NSA will continue to monitor [redacted] and other upstream Section 702 collection systems [redacted] ~~(TS//SI//NF)~~

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

Plaintiff's Exhibit 23



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

FIRST SECTION

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

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

JUDGMENT

STRASBOURG

13 September 2018

Request for referral to the Grand Chamber pending

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



TABLE OF CONTENTS

PROCEDURE **1**

THE FACTS **2**

I. THE CIRCUMSTANCES OF THE CASE **2**

A. Background 2

B. The secret surveillance schemes 3

1. Government Communications Headquarters ("GCHQ") 3

2. The United States' National Security Agency ("NSA") 4

(a) PRISM 4

(b) Upstream 4

C. Domestic proceedings in the first and second of the joined cases 5

D. Domestic proceedings in the third of the joined cases 5

1. The hearing 6

2. The IPT's first judgment of 5 December 2014 8

(a) The PRISM issue 8

(b) The section 8(4) issue 11

3. The IPT's second judgment of 6 February 2015 14

4. The IPT's third judgment of 22 June 2015 as amended by its 1 July 2015 letter 15

II. RELEVANT DOMESTIC LAW AND PRACTICE **16**

A. The interception of communications 16

1. Warrants: general 16

2. Warrants: section 8(4) 18

(a) Authorisation 18

(b) "External" communications 18

3. Specific safeguards under RIPA 19

(a) Section 15 19

(b) Section 16 20

4. The Interception of Communications Code of Practice 22

5. Statement of Charles Farr 35

6. Belhadj and Others v. Security Service, Secret Intelligence Service, Government Communications Headquarters, the Secretary of State for the Home Department, and the Secretary of State for the Foreign and Commonwealth Office, IPT/13/132-9/H and IPT/14/86/CH 35

B. Intelligence sharing 36

1. British-US Communication Intelligence Agreement 36

2. Relevant statutory framework for the operation of the intelligence services 36

(a) MI5 37

(b) MI6 37

(c) GCHQ 37
(d) Counter-Terrorism Act 2008 38
(e) The Data Protection Act 1998 ("DPA") 38
(f) The Official Secrets Act 1989 ("OSA") 38
(g) The Human Rights Act 1998 ("HRA") 39
3. The Interception of Communications Code of Practice 39
C. Acquisition of communications data 40
1. Chapter II of RIPA 40
2. The Acquisition and Disclosure of Communications Data: Code of Practice 41
3. News Group and Others v. The Commissioner of Police of the Metropolis IPT/14/176/H, 17 December 2015 69
4. The Police and Criminal Evidence Act 1984 71
D. IPT practice and procedure 71
1. RIPA 71
2. The Investigatory Powers Tribunal Rules 2000 ("the Rules") 72
3. IPT ruling on preliminary issues of law 73
4. Counsel to the Tribunal 75
E. Oversight 75
F. Reviews of interception operations by the intelligence service 76
1. Intelligence and Security Committee of Parliament: July 2013 Statement on GCHQ's alleged interception of communications under the US PRISM programme 76
2. Privacy and security: a modern and transparent legal framework 77
3. "A Question of Trust": Report of the Investigatory Powers Review by the Independent Reviewer of Terrorism Legislation ("the Anderson Report") 79
4. A Democratic Licence to Operate: Report of the Independent Surveillance Review ("ISR") 81
5. Report of the Bulk Powers Review 82
6. Attacks in London and Manchester March-June 2017: Independent Assessment of MI5 and Police Internal Reviews 83
7. Annual Report of the Interception of Communications Commissioner for 2016 85
(a) Section 8(4) warrants 85
(b) Acquisition of communications data under Chapter II of RIPA 88
G. The Investigatory Powers Act 2016 89
H. Relevant international law 91
1. The United Nations 91
(a) Resolution no. 68/167 on The Right to Privacy in the Digital Age 91
(b) The Constitution of the International Telecommunication Union 1992 91
(c) The 2006 Annual Report of the International Law Commission 91

2. The Council of Europe....93
(a) The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981 93
(b) The Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows of 8 November 2001 (CETS No. 181) 95
(c) Recommendation of the Committee of Ministers on the protection of personal data in the area of telecommunication services....96
(d) The 2001 (Budapest) Convention on Cybercrime....96
(e) The 2015 Report of the European Commission for Democracy through Law ("the Venice Commission") on the Democratic Oversight of Signals Intelligence Agencies 99
I. European Union law....100
1. Charter of Fundamental Rights of the European Union 100
Article 7 – Respect for private and family life 100
Article 8 – Protection of personal data 100
Article 11 – Freedom of expression and information 100
2. EU directives and regulations relating to protection and processing of personal data 100
3. Relevant case-law of the Court of Justice of the European Union ("CJEU")....103
(a) *Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources and Others and Seitinger and Others* (Cases C‑293/12 and C-594/12; ECLI:EU:C:2014:238) 103
(b) *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* (Cases C-203/15 and C-698/15; ECLI:EU:C:2016:970)....105
(c) *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service and Secret Intelligence Service* (IPT/15/110/CH; EU OJ C 22, 22.1.2018, p. 29–30)....106

THE LAW 107

I. EXHAUSTION OF DOMESTIC REMEDIES 107

A. The parties' submissions 107

1. The Government 107

2. The applicants 108

B. The submissions of the third party 109

C. The Court's assessment 109

1. General principles 109

2. Application of those principles to the case at hand 111

II. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION 117

A. The section 8(4) regime 118

1. Admissibility 118

2. Merits 118

(a) The parties' submissions 118

(i) The applicants 118

(ii) The Government 120

(b) The submissions of the third parties 124

(i) Article 19 124

(ii) Access Now 124

(iii) ENNHRI 124

(iv) The Helsinki Foundation for Human Rights ("HFHR") 125

(v) The International Commission of Jurists ("ICJ") 125

(vi) Open Society Justice Initiative ("OSJI") 125

(vii) European Digital Rights ("EDRi") and other organisations active in the field of human rights in the information society 125

(viii) The Law Society of England and Wales 126

(c) The Court's assessment 126

(i) General principles relating to secret measures of surveillance, including the interception of communications 126

(ii) Existing case-law on the bulk interception of communications 129

(iii) The test to be applied in the present case 130

B. The intelligence sharing regime 150

1. Admissibility 150

(a) The parties' submissions 150

(b) The Court's assessment 151

2. Merits 153

(a) The parties' submissions 153

(i) The applicants 153

(ii) The Government 153

(b) The submissions of the third parties 155

(i) The Electronic Privacy Information Center ("EPIC") 155
(ii) Access Now.....155
(iii) Bureau Brandeis.....155
(iv) Center for Democracy and Technology ("CDT") and Pen American Center ("PEN America").....156
(v) The International Commission of Jurists ("ICJ").....156
(vi) Open Society Justice Initiative ("OSJI").....156
(vii) The Law Society of England and Wales.....156
(viii) Human Rights Watch ("HRW").....157
(c) The Court's assessment.....157
(i) The scope of the applicants' complaints.....157
(ii) The nature of the interference.....158
(iii) The applicable test.....158
(iv) Application of the test to material falling into the second category.....160
(v) Application of the test to material falling into the third category.....165
C. The Chapter II regime.....166
1. Admissibility.....166
2. Merits.....167
(a) The parties' submissions.....167
(i) The applicants.....167
(ii) The Government.....168
(b) The Court's assessment.....168
(i) Existing case-law on the acquisition of communications data.....168
(ii) The approach to be taken in the present case.....169
(iii) Examination of the Chapter II regime.....170

III. ALLEGED VIOLATION OF ARTICLE 10 OF THE CONVENTION.....170

A. Admissibility.....171
1. The applicants in the third of the joined cases.....171
2. The applicants in the second of the joined cases.....172
B. Merits.....172
1. The parties' submissions.....172
(a) The applicants.....172
(b) The Government.....173
2. The submissions of the third parties.....174
(a) The Helsinki Foundation for Human Rights.....174
(b) The National Union of Journalists ("NUJ") and the International Federation of Journalists ("IFJ").....174
(c) The Media Lawyers' Association ("MLA").....175

3. The Court's assessment 175
(a) General principles....175
(b) The application of the general principles to the present case....176
(i) The section 8(4) regime....176
(ii) The Chapter II regime 178
(iii) Overall conclusion 179

IV. ALLEGED VIOLATION OF ARTICLE 6 OF THE CONVENTION....179

V. ALLEGED VIOLATION OF ARTICLE 14 OF THE CONVENTION COMBINED WITH ARTICLES 8 AND 10 OF THE CONVENTION 181

VI. APPLICATION OF ARTICLE 41 OF THE CONVENTION....183
A. Damage 183
B. Costs and expenses....183
C. Default interest....183

FOR THESE REASONS, THE COURT:....184

APPENDIX....186

PARTLY CONCURRING, PARTLY DISSENTING OPINION OF JUDGE KOSKELO, JOINED BY JUDGE TURKOVIĆ....187
I. The RIPA section 8(4) regime....187
(i) The context of earlier case-law 187
(ii) The context of the present case 189
(iii) Concerns....190
II. The intelligence-sharing regime....194

JOINT PARTLY DISSENTING AND PARTLY CONCURRING OPINION OF JUDGES PARDALOS AND EICKE....195
Introduction 195
Admissibility 196
The section 8(4) regime 199
Post Scriptum....203

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

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

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

and Abel Campos, *Section Registrar,*

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

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

PROCEDURE

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

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

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

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

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

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

There appeared before the Court:

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

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

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

THE FACTS

I. THE CIRCUMSTANCES OF THE CASE

A. Background

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

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

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

B. The secret surveillance schemes

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

1. Government Communications Headquarters ("GCHQ")

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

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

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

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

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

14. The legal framework for bulk interception in force at the relevant time is set out in detail in the "Relevant Domestic law and practice" section below. In brief, section 8(4) of the Regulation of Investigatory Powers Act 2000 ("RIPA" – see paragraph 67 below) allows the Secretary of State to issue warrants for the "interception of external communications", and pursuant to section 16 of RIPA (see paragraphs 78-85 below) intercepted material cannot be selected to be read, looked at or listened to, "according to a factor which is referable to an individual who is known to be for the time being in the British Islands".

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

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

(a) PRISM

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

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

(b) Upstream

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

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

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

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

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

D. Domestic proceedings in the third of the joined cases

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

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

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

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

1. The hearing

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(a) The PRISM issue

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

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

33. The IPT continued:

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

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

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

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

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

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

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

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

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

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

"(i) Having considered the arrangements below the waterline, as described in this judgment, we are satisfied that there are adequate arrangements in place for the purpose of ensuring compliance with the statutory framework and with Articles 8 and 10 of the Convention, so far as the receipt of intercept from Prism and/or Upstream is concerned.

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

(iii) These arrangements are subject to oversight.

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

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

(b) The section 8(4) issue

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

II. RELEVANT DOMESTIC LAW AND PRACTICE

A. The interception of communications

1. Warrants: general

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

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

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

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

59. Section 81(5) provides:

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

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

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

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

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

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

> "(a) any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;
>
> (b) any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person—
>
> i. of any postal service or telecommunications service; or
>
> ii. in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;
>
> (c) any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service."

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

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

2. Warrants: section 8(4)

(a) Authorisation

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

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

(b) "External" communications

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

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

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

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

3. Specific safeguards under RIPA

(a) Section 15

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

73. Section 15(2) provides:

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

74. Section 15(3) provides:

> "The requirements of this subsection are satisfied in relation to the intercepted material and any related communications data if each copy made of any of the material or data (if not destroyed earlier) is destroyed as soon as there are no longer any grounds for retaining it as necessary for any of the authorised purposes."

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

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

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

77. Pursuant to section 15(6), the arrangements to which section 15(1) refers are not required to secure that the requirements of section 15(2) and (3) are satisfied in so far as they relate to any of the intercepted material or related communications data, or any copy of any such material or data, possession of which has been surrendered to any authorities of a country or territory outside the United Kingdom. However, such arrangements are required to secure, in the case of every such warrant, that possession of the intercepted material and data and of copies of the material or data is surrendered to authorities of a country or territory outside the United Kingdom only if the requirements of section 15(7) are satisfied. Section 15(7) provides:

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

(b) Section 16

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

79. Section 16(2) provides:

> "Subject to subsections (3) and (4), intercepted material falls within this subsection so far only as it is selected to be read, looked at or listened to otherwise than according to a factor which–
>
> (a) is referable to an individual who is known to be for the time being in the British Islands; and
>
> (b) has as its purpose, or one of its purposes, the identification of material contained in communications sent by him, or intended for him."

80. Pursuant to section 16(3), intercepted material falls within section 16(2), notwithstanding that it is selected by reference to one of the factors mentioned in that subsection, if it is certified by the Secretary of State for the purposes of section 8(4) that the examination of material selected according to factors referable to the individual in question is necessary as mentioned in subsection 5(3) of the Act; and the material relates only to communications sent during a period specified in the certificate that is no longer than the permitted maximum.

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

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

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

83. Section 16(5) provides:

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

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

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

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

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

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

4. The Interception of Communications Code of Practice

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

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

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

90. Insofar as relevant, the IC Code provides:

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

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

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

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

Necessity and proportionality

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

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

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

3.7. The following elements of proportionality should therefore be considered:

- Balancing the size and scope of the proposed interference against what is sought to be achieved;
- Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- Evidencing, as far as reasonably practicable, what other methods have been considered and were either not implemented or have been employed but which are assessed as insufficient to fulfil operational objectives without the addition of the intercept material sought.

...

Duration of interception warrants

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

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

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

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

...

4. SPECIAL RULES ON INTERCEPTION WITH A WARRANT

Collateral intrusion

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

Confidential information

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

4.3. Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking. See also paragraphs 4.26 and 4.28 – 4.31 for additional safeguards that should be applied in respect of confidential journalistic material.

...

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

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

...

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

4.29. Material which has been identified as confidential information should be retained only where it is necessary and proportionate to do so for one or more of the authorised purposes set out in section 15(4). It must be securely destroyed when its retention is no longer needed for those purposes. If such information is retained, there must be adequate information management systems in place to ensure that continued retention remains necessary and proportionate for the authorised statutory purposes.

4.30. Where confidential information is retained or disseminated to an outside body, reasonable steps should be taken to mark the information as confidential. Where there is any doubt as to the lawfulness of the proposed handling or dissemination of confidential information, advice should be sought from a legal adviser within the relevant intercepting agency and before any further dissemination of the material takes place.

4.31. Any case where confidential information is retained should be notified to the Interception of Communications Commissioner as soon as reasonably practicable, as agreed with the Commissioner. Any material which has been retained should be made available to the Commissioner on request.

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

...

6. INTERCEPTION WARRANTS (SECTION 8(4))

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

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

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

Section 8(4) interception in practice

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

Definition of external communications

6.5. External communications are defined by RIPA to be those which are sent or received outside the British Islands. They include those which are both sent and received outside the British Islands, whether or not they pass through the British Islands in the course of their transmission. They do not include communications both sent and received in the British Islands, even if they pass outside the British Islands en

route. For example, an email from a person in London to a person in Birmingham will be an internal, not external communication for the purposes of section 20 of RIPA, whether or not it is routed via IP addresses outside the British Islands, because the sender and intended recipient are within the British Islands.

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

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

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

Application for a section 8(4) warrant

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

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

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

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

- An assurance that intercepted material will be read, looked at or listened to only so far as it is certified and it meets the conditions of sections 16(2)-16(6) of RIPA; and
- An assurance that all material intercepted will be handled in accordance with the safeguards required by sections 15 and 16 of RIPA (see paragraphs 7.2 and 7.10 respectively).

Authorisation of a section 8(4) warrant

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

- In the interests of national security;
- For the purpose of preventing or detecting serious crime; or
- For the purpose of safeguarding the economic well-being of the UK so far as those interests are also relevant to the interests of national security.

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

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

6.14. When the Secretary of State issues a warrant of this kind, it must be accompanied by a certificate in which the Secretary of State certifies that he or she considers examination of the intercepted material to be necessary for one or more of the section 5(3) purposes. The purpose of the statutory certificate is to ensure that a selection process is applied to intercepted material so that only material described in the certificate is made available for human examination. Any certificate must broadly reflect the "Priorities for Intelligence Collection" set by the NSC for the guidance of the intelligence agencies. For example, a certificate might provide for the examination of material providing intelligence on terrorism (as defined in the Terrorism Act 2000) or on controlled drugs (as defined by the Misuse of Drugs Act 1971). The Interception of Communications Commissioner must review any changes to the descriptions of material specified in a certificate.

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

Urgent authorisation of a section 8(4) warrant

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

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

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

Format of a section 8(4) warrant

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

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

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

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

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

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

Renewal of a section 8(4) warrant

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

update of the matters outlined in paragraph 6.10 above. In particular, the applicant must give an assessment of the value of interception to date and explain why it is considered that interception continues to be necessary for one or more of the purposes in section 5(3), and why it is considered that interception continues to be proportionate.

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

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

Warrant cancellation

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

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

Records

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

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

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

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

7. SAFEGUARDS

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

The section 15 safeguards

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

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

Dissemination of intercepted material

7.3. The number of persons to whom any of the intercepted material is disclosed, and the extent of disclosure, is limited to the minimum that is necessary for the authorised purposes set out in section 15(4) of RIPA. This obligation applies equally to disclosure to additional persons within an agency, and to disclosure outside the agency. It is enforced by prohibiting disclosure to persons who have not been appropriately vetted and also by the need-to-know principle: intercepted material must not be disclosed to any person unless that person's duties, which must relate to one of the authorised purposes, are such that he or she needs to know about the intercepted material to carry out those duties. In the same way, only so much of the intercepted

material may be disclosed as the recipient needs. For example, if a summary of the intercepted material will suffice, no more than that should be disclosed.

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

7.5. Where intercepted material is disclosed to the authorities of a country or territory outside the UK, the agency must take reasonable steps to ensure that the authorities in question have and will maintain the necessary procedures to safeguard the intercepted material, and to ensure that it is disclosed, copied, distributed and retained only to the minimum extent necessary. In particular, the intercepted material must not be further disclosed to the authorities of a third country or territory unless explicitly agreed with the issuing agency, and must be returned to the issuing agency or securely destroyed when no longer needed.

Copying

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

Storage

7.7. Intercepted material and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of vetting. This requirement to store intercept product securely applies to all those who are responsible for handling it, including CSPs. The details of what such a requirement will mean in practice for CSPs will be set out in the discussions they have with the Government before a Section 12 Notice is served (see paragraph 3.13).

Destruction

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

7.9. Where an intercepting agency undertakes interception under a section 8(4) warrant and receives unanalysed intercepted material and related communications data from interception under that warrant, the agency must specify (or must determine on a system by system basis) maximum retention periods for different categories of the data which reflect its nature and intrusiveness. The specified periods should normally be no longer than two years, and should be agreed with the Interception of Communications Commissioner. Data may only be retained for longer than the applicable maximum retention periods if prior authorisation is obtained from a senior official within the particular intercepting agency on the basis that continued retention

of the data has been assessed to be necessary and proportionate. If continued retention of any such data is thereafter assessed to no longer meet the tests of necessity and proportionality, it must be deleted. So far as possible, all retention periods should be implemented by a process of automated deletion, which is triggered once the applicable maximum retention period has been reached for the data at issue.

Personnel security

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

The section 16 safeguards

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

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

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

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

7.14. In general, automated systems must, where technically possible, be used to effect the selection in accordance with section 16(1) of RIPA. As an exception, a certificate may permit intercepted material to be accessed by a limited number of specifically authorised staff without having been processed or filtered by the automated systems. Such access may only be permitted to the extent necessary to determine whether the material falls within the main categories to be selected under the certificate, or to ensure that the methodology being used remains up to date and effective. Such checking must itself be necessary on the grounds specified in section 5(3) of RIPA. Once those functions have been fulfilled, any copies made of the material for those purposes must be destroyed in accordance with section 15(3) of RIPA. Such checking by officials should be kept to an absolute minimum; whenever possible, automated selection techniques should be used instead. Checking will be kept under review by the Interception of Communications Commissioner during his or her inspections.

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

safeguards. All authorised persons must be appropriately vetted (see paragraph 7.10 for further information).

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

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

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

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

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

...

10. OVERSIGHT

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

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

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

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

5. Statement of Charles Farr

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

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

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

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

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

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

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

B. Intelligence sharing

1. British-US Communication Intelligence Agreement

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

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

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

(a) MI5

98. Pursuant to section 2 of the Security Services Act 1989 ("SSA"), it is the duty of the Director-General of MI5, who is appointed by the Secretary of State, to ensure that there are arrangements for securing that no information is obtained by MI5 except so far as necessary for the proper discharge of its functions or disclosed by it except so far as necessary for that purpose or for the purpose of the prevention or detection of serious crime or for the purpose of any criminal proceedings.

99. According to section 1 of the SSA, the functions of MI5 are the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means; to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands; and to act in support of the activities of police forces, the National Crime Agency and other law enforcement agencies in the prevention and detection of serious crime.

(b) MI6

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

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

(c) GCHQ

102. Section 4 of the ISA provides that it is the duty of the Director of GCHQ, who is appointed by the Secretary of State, to ensure that there are arrangements for securing that it obtains no information except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary.

103. According to section 3 of the ISA, one of the functions of GCHQ is to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material. This function is exercisable only in the interests of national security, with particular reference to the State's defence and foreign policies; in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or in support of the prevention or detection of serious crime.

(d) Counter-Terrorism Act 2008

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

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

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

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

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

and

> "(7) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

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

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

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

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

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

3. The Interception of Communications Code of Practice

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

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

Application of this chapter

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

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

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

- A relevant interception warrant under RIPA has already been issued by the Secretary of State, the assistance of the foreign government is necessary to obtain the particular communications because they cannot be obtained under the relevant RIPA interception warrant and it is necessary and proportionate for the intercepting agency to obtain those communications; or
- Making the request for the particular communications in the absence of a relevant RIPA interception warrant does not amount to a deliberate circumvention of RIPA or otherwise frustrate the objectives of RIPA (for example, because it is not technically feasible to obtain the communications via RIPA interception), and it is necessary and proportionate for the intercepting agency to obtain those communications.

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

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

"descriptions of intercepted material" covering the subject's communications (for other individuals).

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

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

12.6. Where intercepted communications content or communications data are obtained by the intercepting agencies as set out in paragraph 12.2, or are otherwise received by them from the government of a country or territory outside the UK in circumstances where the material identifies itself as the product of an interception, (except in accordance with an international mutual assistance agreement), the communications content and communications data must be subject to the same internal rules and safeguards that apply to the same categories of content or data when they are obtained directly by the intercepting agencies as a result of interception under RIPA.

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

C. Acquisition of communications data

1. Chapter II of RIPA

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

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

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

"(a) in the interests of national security;

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

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

(d) in the interests of public safety;

(e) for the purpose of protecting public health;

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

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

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

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

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

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

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

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

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

"**1 INTRODUCTION**

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

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

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

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

...

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

...

2 GENERAL EXTENT OF POWERS

Scope of Powers, Necessity and Proportionality

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Communications Data

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

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

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

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

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

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

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

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

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

2.21. Communications data is defined as:

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

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

...

Traffic Data

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

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

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

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

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

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

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

...

Service Use Information

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

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

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

Subscriber Information

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

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

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

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

...

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

Further Guidance on Necessity and Proportionality

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

Necessity

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

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

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

Proportionality

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The applicant

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

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

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

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

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

The designated person

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

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

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

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

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

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

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

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

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

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

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

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

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

...

The single point of contact

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

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

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

3.22. The SPoC should be in a position to:

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

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

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

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

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

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

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

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

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

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

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

The senior responsible officer

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

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

Authorisations

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

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

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

3.35. An authorisation may be appropriate where:

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

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

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

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

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

...

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

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

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

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

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

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

Notices

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

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

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

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

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

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

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

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

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

Duration of authorisations and notices

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

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

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

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

Renewal of authorisations and notices

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

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

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

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

Cancellation of notices and withdrawal of authorisations

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

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

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

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

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

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

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

3.63. Withdrawal of an authorisation should:

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

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

Urgent oral giving of notice or grant of authorisation

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

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

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

...

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

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

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

Communications data involving certain professions

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

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

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

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

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

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

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

Applications to determine the source of journalistic information

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

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

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

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

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

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

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

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

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

Local authority authorisation procedure

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

...

6 KEEPING OF RECORDS

Records to be kept by a relevant public authority

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

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

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

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

...

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

I. the CSP from whom the data is being acquired.

6.7. These records must be sent in written or electronic form to the Commissioner, as determined by him. Guidance on record keeping will be issued by IOCCO. Guidance may also be sought by relevant public authorities, CSPs or persons contracted by them to develop or maintain their information technology systems.

6.8. The Interception of Communications Commissioner will not seek to publish statistical information where it appears to him that doing so would be contrary to the public interest, or would be prejudicial to national security.

Records to be kept by a Communications Service Provider

6.9. To assist the Commissioner to carry out his statutory function in relation to Chapter II, CSPs should maintain a record of the disclosures it has made or been required to make. This record should be available to the Commissioner and his inspectors to enable comparative scrutiny of the records kept by public authorities. Guidance on the maintenance of records by CSPs may be issued by or sought from IOCCO.

6.10. The records to be kept by a CSP, in respect of each notice or authorisation, should include:

A. the name of the public authority;

B. the URN of the notice or authorisation;

C. the date the notice was served upon the CSP or the authorisation disclosed to the CSP;

D. a description of any communications data required where no disclosure took place or could have taken place;

E. the date when the communications data was made available to the public authority or, where secure systems are provided by the CSP, the date when the acquisition and disclosure of communications data was undertaken; and

F. sufficient records to establish the origin and exact communications data that has been disclosed in the event of later challenge in court.

Errors

6.11. Proper application of RIPA and thorough procedures for operating its provisions, including the careful preparation and checking of applications, notices and authorisations, should reduce the scope for making errors whether by public authorities or by CSPs.

6.12. An error can only occur after a designated person:

- has granted an authorisation and the acquisition of data has been initiated; or
- has given notice and the notice has been served on a CSP in writing, electronically or orally.

6.13. Any failure by a public authority to apply correctly the process of acquiring or obtaining communications data set out in this code will increase the likelihood of an error occurring.

6.14. Where any error occurs in the grant of an authorisation, the giving of a notice or as a consequence of any authorised conduct, or any conduct undertaken to comply with a notice, a record should be kept.

6.15. Where an error results in communications data being acquired or disclosed wrongly, a report must be made to the Commissioner ('a reportable error'). Such errors can have very significant consequences on an affected individual's rights with details of their private communications being disclosed to a public authority and, in extreme circumstances, being wrongly detained or wrongly accused of a crime as a result of that error.

6.16. In cases where an error has occurred but is identified by the public authority or the CSP without data being acquired or disclosed wrongly, a record will be maintained by the public authority of such occurrences ('recordable error'). These records must be available for inspection by the Commissioner.

6.17. This section of the code cannot provide an exhaustive list of possible causes of reportable or recordable errors. Examples could include:

Reportable errors

- an authorisation or notice made for a purpose, or for a type of data, which the relevant public authority cannot call upon, or seek, under RIPA;
- human error, such as incorrect transposition of information from an application to an authorisation or notice where communications data is acquired or disclosed;
- disclosure of the wrong data by a CSP when complying with a notice; and
- acquisition of the wrong data by a public authority when engaging in conduct specified in an authorisation.

Recordable errors

- a notice has been given which is impossible for a CSP to comply with and the public authority attempts to impose the requirement;
- failure to review information already held, for example unnecessarily seeking the acquisition or disclosure of data already acquired or obtained for the same investigation or operation;
- the requirement to acquire or obtain the data is known to be no longer valid;
- failure to serve written notice (or where appropriate an authorisation) upon a CSP within one working day of urgent oral notice being given or an urgent oral authorisation granted; and

- human error, such as incorrect transposition of information from an application to an authorisation or notice where communications data is not acquired or disclosed.

6.18. Reporting and recording of errors will draw attention to those aspects of the process of acquisition and disclosure of communications data that require further improvement to eliminate errors and the risk of undue interference with any individual's rights.

6.19. When a reportable error has been made, the public authority which made the error, or established that the error had been made, must establish the facts and report the error to the authority's senior responsible officer and then to the IOCCO within no more than five working days of the error being discovered. All errors should be reported as they arise. If the report relates to an error made by a CSP, the public authority should also inform the CSP and IOCCO of the report in written or electronic form. This will enable the CSP and IOCCO to investigate the cause or causes of the reported error.

6.20. The report sent to the IOCCO by a public authority in relation to a reportable error must include details of the error, identified by the public authority's unique reference number of the relevant authorisation or notice, explain how the error occurred, indicate whether any unintended collateral intrusion has taken place and provide an indication of what steps have been, or will be, taken to ensure that a similar error does not recur. When a public authority reports an error made by a CSP, the report must include details of the error and indicate whether the CSP has been informed or not (in which case the public authority must explain why the CSP has not been informed of the report).

6.21. Where a CSP discloses communications data in error, it must report each error to the IOCCO within no more than five working days of the error being discovered. It is appropriate for a person holding a suitably senior position within a CSP to do so, identifying the error by reference to the public authority's unique reference number and providing an indication of what steps have been, or will be, taken to ensure that a similar error does not recur. Errors by service providers could include responding to a notice by disclosing incorrect data or by disclosing the required data to the wrong public authority.

6.22. In circumstances where a reportable error is deemed to be of a serious nature, the Commissioner may investigate the circumstances that led to the error and assess the impact of the interference on the affected individual's rights. The Commissioner may inform the affected individual, who may make a complaint to the Investigatory Powers Tribunal (see section 9).

6.23. The records kept by a public authority accounting for recordable errors must include details of the error, explain how the error occurred and provide an indication of what steps have been, or will be, taken to ensure that a similar error does not reoccur. The authority's senior responsible officer must undertake a regular review of the recording of such errors.

6.24. Where material which has no connection or relevance to any investigation or operation undertaken by the public authority receiving it is disclosed in error by a CSP, that material and any copy of it (including copies contained in or as attachments in electronic mail) should be destroyed as soon as the report to the Commissioner has been made.

...

Excess Data

6.26. Where authorised conduct by a public authority results in the acquisition of excess data, or its disclosure by a CSP in order to comply with the requirement of a notice, all the data acquired or disclosed should be retained by the public authority.

6.27. Where a public authority is bound by the CPIA and its code of practice, there will be a requirement to record and retain data which is relevant to a criminal investigation, even if that data was disclosed or acquired beyond the scope of a valid notice or authorisation. If a criminal investigation results in proceedings being instituted all material that may be relevant must be retained at least until the accused is acquitted or convicted or the prosecutor decides not to proceed.

6.28. If, having reviewed the excess data, it is intended to make use of the excess data in the course of the investigation or operation, an applicant must set out the reason(s) for needing to use that material in an addendum to the application upon which the authorisation or notice was originally granted or given. The designated person will then consider the reason(s) and review all the data and consider whether it is necessary and proportionate for the excess data to be used in the investigation or operation. As with all communications data acquired, the requirements of the DPA and its data protection principles must also be adhered to in relation to any excess data (see next section).

7 DATA PROTECTION SAFEGUARDS

7.1. Communications data acquired or obtained under the provisions of RIPA, and all copies, extracts and summaries of it, must be handled and stored securely. In addition, the requirements of the DPA and its data protection principles must be adhered to.

7.2. Communications data that is obtained directly as a consequence of the execution of an interception warrant must be treated in accordance with the safeguards which the Secretary of State has approved in accordance with section 15 of RIPA.

Disclosure of communications data and subject access rights

7.3. This section of the code provides guidance on the relationship between disclosure of communications data under RIPA and the provisions for subject access requests under the DPA, and the balance between CSPs' obligations to comply with a notice to disclose data and individuals' right of access under section 7 of the DPA to personal data held about them.

7.4. There is no provision in RIPA preventing CSPs from informing individuals about whom they have been required by notice to disclose communications data in response to a Subject Access Request made under section 7 of the DPA. However a CSP may exercise certain exemptions to the right of subject access under Part IV of the DPA.

7.5. Section 28 of the DPA provides that data are always exempt from section 7 where such an exemption is required for the purposes of safeguarding national security.

7.6. Section 29 of the DPA provides that personal data processed for the purposes of the prevention and detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty or other imposition of a similar nature are exempt from section 7 to the extent to which the application of the provisions for rights of data subjects would be likely to prejudice any of those matters.

7.7. The exemption to subject access rights possible under section 29 does not automatically apply to the disclosure of the existence of notices given under RIPA. In the event that a CSP receives a subject access request where the fact of a disclosure under RIPA might itself be disclosed, the CSP concerned must carefully consider whether in the particular case disclosure of the fact of the notice would be likely to prejudice the prevention or detection of crime.

7.8. Where a CSP is uncertain whether disclosure of the fact of a notice would be likely to prejudice an investigation or operation, it should approach the SPoC of the public authority which gave the notice – and do so in good time to respond to the subject access request. The SPoC can make enquiries within the public authority to determine whether disclosure of the fact of the notice would likely be prejudicial to the matters in section 29.

7.9. Where a CSP withholds a piece of information in reliance on the exemption in section 28 or 29 of the DPA, it is not obliged to inform an individual that any information has been withheld. It can simply leave out that piece of information and make no reference to it when responding to the individual who has made the subject access request.

7.10. CSPs should keep a record of the steps they have taken in determining whether disclosure of the fact of a notice would prejudice the apprehension or detection of offenders. This might be useful in the event of the data controller having to respond to enquiries made subsequently by the Information Commissioner, the courts and, in the event of prejudice, the police. Under section 42 of the DPA an individual may request that the Information Commissioner assesses whether a subject access request has been handled in compliance with the DPA.

Acquisition of communication data on behalf of overseas authorities

7.11. While the majority of public authorities which obtain communications data under RIPA have no need to disclose that data to any authority outside the United Kingdom, there can be occasions when it is necessary, appropriate and lawful to do so in matters of international co‑operation.

7.12. There are two methods by which communications data, whether obtained under RIPA or not, can be acquired and disclosed to overseas public authorities:

- judicial co‑operation; or
- non‑judicial co‑operation.

Neither method compels United Kingdom public authorities to disclose data to overseas authorities. Data can only be disclosed when a United Kingdom public authority is satisfied that it is in the public interest to do so and all relevant conditions imposed by domestic legislation have been fulfilled.

Judicial co-operation

7.13. A central authority in the United Kingdom may receive a request for mutual legal assistance (MLA) which includes a request for communications data from an overseas court exercising criminal jurisdiction, an overseas prosecuting authority, or any other overseas authority that appears to have a function of making requests for MLA. This MLA request must be made in connection with criminal proceedings or a criminal investigation being carried on outside the United Kingdom, and the request for communications data included must be capable of satisfying the requirements of Part I Chapter II of RIPA.

7.14. If such an MLA request is accepted by the central authority, it will be referred for consideration by the appropriate public authority in the UK. The application may then be considered and, if appropriate, executed by that public authority under section 22 of RIPA and in line with the guidance in this code of practice.

7.15. In order for a notice or authorisation to be granted, the United Kingdom public authority must be satisfied that the application meets the same criteria of necessity and proportionality as required for a domestic application.

Non-judicial co-operation

7.16. Public authorities in the United Kingdom can receive direct requests for assistance from their counterparts in other countries. These can include requests for the acquisition and disclosure of communications data for the purpose of preventing or detecting crime. On receipt of such a request, the United Kingdom public authority may consider seeking the acquisition or disclosure of the requested data under the provisions of Chapter II of Part I of RIPA.

7.17. The United Kingdom public authority must be satisfied that the request complies with United Kingdom obligations under human rights legislation. The necessity and proportionality of each case must be considered before the authority processes the authorisation or notice.

Disclosure of communications data to overseas authorities

7.18. Where a United Kingdom public authority is considering the acquisition of communications data on behalf of an overseas authority and transferring the data to that authority, it must consider whether the data will be adequately protected outside the United Kingdom and what safeguards may be needed to ensure that. Such safeguards might include attaching conditions to the processing, storage and destruction of the data.

7.19. If the proposed transfer of data is to an authority within the European Union, that authority will be bound by the European Data Protection Directive (95/46/EC) and its national data protection legislation. Any data disclosed will be protected there without need for additional safeguards.

7.20. If the proposed transfer is to an authority outside of the European Union and the European Economic Area (Iceland, Liechtenstein and Norway), then it must not be disclosed unless the overseas authority can ensure an adequate level of data protection. The European Commission has determined that certain countries, for example Switzerland, have laws providing an adequate level of protection where data can be transferred without need for further safeguards.

7.21. In all other circumstances, the United Kingdom public authority must decide in each case, before transferring any data overseas, whether the data will be adequately protected there. The Information Commissioner has published guidance on sending personal data outside the European Economic Area in compliance with the Eighth Data Protection Principle, and, if necessary, his office can provide guidance.

7.22. The DPA recognises that it will not always be possible to ensure adequate data protection in countries outside of the European Union and the European Economic Area, and there are exemptions to the principle, for example if the transfer of data is necessary for reasons of 'substantial public interest'. There may be circumstances when it is necessary, for example in the interests of national security, for communications data to be disclosed to a third party country, even though that country does not have adequate safeguards in place to protect the data. That is a

decision that can only be taken by the public authority holding the data on a case by case basis.

8 OVERSIGHT

8.1. RIPA provides for an Interception of Communications Commissioner ('the Commissioner') whose remit is to provide independent oversight of the exercise and performance of the powers and duties contained under Chapter II of Part I of RIPA. The Commissioner is supported by his inspectors who work from the Interception of Communications Commissioner's Office (IOCCO).

8.2. This code does not cover the exercise of the Commissioner's functions. It is the duty of any person who uses the powers conferred by Chapter II, or on whom duties are conferred, to comply with any request made by the Commissioner to provide any information he requires for the purposes of enabling him to discharge his functions.

8.3. Should the Commissioner establish that an individual has been adversely affected by any wilful or reckless failure by any person within a relevant public authority exercising or complying with the powers and duties under RIPA in relation to the acquisition or disclosure of communications data, he shall, subject to safeguarding national security, inform the affected individual of the existence of the Tribunal and its role. The Commissioner should disclose sufficient information to the affected individual to enable them to engage the Tribunal effectively.

8.4. Reports made by the Commissioner concerning the inspection of public authorities and their exercise and performance of powers under Chapter II may be made available by the Commissioner to the Home Office to promulgate good practice and help identify training requirements within public authorities and CSPs.

8.5. Subject to the approval of the Commissioner, public authorities may publish their inspection reports, in full or in summary, to demonstrate both the oversight to which they are subject and their compliance with Chapter II of RIPA and this code. Approval should be sought on a case by case basis at least ten working days prior to intended publication, stating whether the report is to be published in full, and, if not, stating which parts are to be published or how it is to be summarised."

3. News Group and Others v. The Commissioner of Police of the Metropolis IPT/14/176/H, 17 December 2015

118. These proceedings were brought before the IPT by three journalists and their employer. They challenged four authorisations issued under section 22 of RIPA with the purpose of enabling police to obtain communications data which might reveal sources of information obtained by the journalists. They argued, *inter alia*, that the section 22 regime (at the time supplemented by the 2007 Code of Practice) breached their rights under Article 10 of the Convention as it did not adequately safeguard the confidentiality of journalists' sources. The IPT agreed that the regime in place at the time did not contain effective safeguards to protect Article 10 rights in a case in which the authorisation had the purpose of obtaining disclosure of the identity of a journalist's source. It held:

"107. In the absence of a requirement for prior scrutiny by a court, particular regard must be paid to the adequacy of the other safeguards prescribed by the law. The designated person is not independent of the police force, although in practice, properly

complying with the requirements of s 22, he will make an independent judgement, as he did in this case. In general the requirement for a decision on necessity and proportionality to be taken by a senior officer who is not involved in the investigation does provide a measure of protection as to process, but the role of the designated person cannot be equated to that of an independent and impartial judge or tribunal.

108. Subsequent oversight by the Commissioner, or, in the event of a complaint, by this Tribunal, cannot after the event prevent the disclosure of a journalist's source. This is in contrast to criminal investigations where a judge at a criminal trial may be able to exclude evidence which has been improperly or unfairly obtained by an authorisation made under s 22. Where an authorisation is made which discloses a journalist's source that disclosure cannot subsequently be reversed, nor the effect of such disclosure mitigated. Nor was there any requirement in the 2007 Code for any use of s 22 powers for the purpose of obtaining disclosure of a journalist's source to be notified to the Commissioner, so in such cases this use of the power might not be subject to any effective review. Furthermore none of the Complainants had any reason to suspect that their data had been accessed until the closing report on Operation Alice was published in September 2014. If the Respondent had not disclosed that information – and it is to his credit that he did – then the Complainants would never have been in a position to bring these proceedings.

109. So in a case involving the disclosure of a journalist's source the safeguards provided for under s 22 and the 2007 Code were limited to requiring a decision as to necessity and proportionality to be made by a senior police officer, who was not directly involved in the investigation and who had a general working knowledge of human rights law. The 2007 Code imposed no substantive or procedural requirement specific to cases affecting the freedom of the press. There was no requirement that an authorisation should only be granted where the need for disclosure was convincingly established, nor that there should be very careful scrutiny balancing the public interest in investigating crime against the protection of the confidentiality of journalistic sources. The effect of s 22 and the 2007 Code was that the designated person was to make his decision on authorisation on the basis of the same general tests of necessity and proportionality which would be applied to an application in any criminal investigation."

119. The IPT could not award any remedy in respect of the failure to provide adequate safeguards to protect Article 10 rights, as this did not in itself render the authorisations unlawful. However, it also found that one of the authorisations was unlawful, as it had been neither proportionate nor necessary. In considering the appropriate remedy, it acknowledged that it had the power to award compensation, but declined to do so since it did not consider it necessary to afford just satisfaction.

120. In March 2015 the 2007 Code of Practice was replaced by a new code. Paragraph 3.78 of that new ACD Code provides that in the specific case of an application for communications data, which is made in order to identify a journalist's source, those law enforcement agencies with powers under the Police and Criminal Evidence Act 1984 (PACE) must use the procedures of PACE to apply to a court for a production order to obtain this data.

4. The Police and Criminal Evidence Act 1984

121. Schedule 1 of PACE governs the procedure for applying to court for a production order. It provides, as relevant:

> "1. If on an application made by a constable a judge is satisfied that one or other of the sets of access conditions is fulfilled, he may make an order under paragraph 4 below.
>
> ...
>
> 4. An order under this paragraph is an order that the person who appears to the judge to be in possession of the material to which the application relates shall—
>
> (a) produce it to a constable for him to take away; or
>
> (b) give a constable access to it,
>
> not later than the end of the period of seven days from the date of the order or the end of such longer period as the order may specify.
>
> ...
>
> 7. An application for an order under paragraph 4 above that relates to material that consists of or includes journalistic material shall be made *inter partes*."

122. Section 78 of PACE permits a court to refuse to allow evidence on which the prosecution proposes to rely to be given if it appears to the court that, having regard to all the circumstances, including the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it.

D. IPT practice and procedure

1. RIPA

123. The IPT was established under section 65(1) of RIPA to hear allegations by citizens of wrongful interference with their communications as a result of conduct covered by that Act. Members must hold or have held high judicial office or be a qualified lawyer of at least ten years' standing.

124. Section 65(2) provides that the IPT is the only appropriate forum in relation to proceedings against any of the intelligence services for acts allegedly incompatible with Convention rights, and complaints by persons who allege to have been subject to the investigatory powers of RIPA. It has jurisdiction to investigate any complaint that a person's communications have been intercepted and, where interception has occurred, to examine the authority for such interception.

125. According to sections 67(2) and 67(3)(c), the IPT is to apply the principles applicable by a court on an application for judicial review. It does not, however, have power to make a Declaration of Incompatibility if it finds primary legislation to be incompatible with the European Convention

on Human Rights as it is not a "court" for the purposes of section 4 of the Human Rights Act 1998.

126. Under section 67(8), there is no appeal from a decision of the IPT "except to such extent as the Secretary of State may by order otherwise provide". No such order has been made by the Secretary of State. Furthermore, in *R(Privacy International) v. Investigatory Powers Tribunal* [2017] EWCA Civ 1868 the Court of Appeal recently confirmed that section 67(8) also had the effect of preventing a judicial review claim from being brought against a decision of the IPT. As a consequence, the IPT is a court of last resort for the purposes of the obligation to request a preliminary ruling under Article 267 of the Treaty on the Functioning of the European Union (see paragraph 236 below).

127. Section 68(6) and (7) requires those involved in the authorisation and execution of an interception warrant to disclose or provide to the IPT all documents and information it may require.

128. Section 68(4) provides that where the IPT determines any complaint it has the power to award compensation and to make such other orders as it thinks fit, including orders quashing or cancelling any warrant and orders requiring the destruction of any records obtained thereunder (section 67(7)). In the event that a claim before the IPT is successful, the IPT is generally required to make a report to the Prime Minister (section 68(5)).

129. Section 68(1) entitles the IPT to determine its own procedure, although section 69(1) provides that the Secretary of State may also make procedural rules.

2. The Investigatory Powers Tribunal Rules 2000 ("the Rules")

130. The Rules were adopted by the Secretary of State to govern various aspects of the procedure before the IPT.

131. Although the IPT is under no duty to hold oral hearings, pursuant to Rule 9 it may hold, at any stage of consideration, oral hearings at which the complainant may make representations, give evidence and call witnesses. It may also hold separate oral hearings which the person whose conduct is the subject of the complaint, the public authority against which the proceedings are brought, or any other person involved in the authorisation or execution of an interception warrant may be required to attend. Rule 9 provides that the IPT's proceedings, including any oral hearings, are to be conducted in private.

132. Rule 11 allows the IPT to receive evidence in any form, even where it would not be admissible in a court of law. It may require a witness to give evidence on oath, but no person can be compelled to give evidence at an oral hearing under Rule 9(3).

133. Rule 13 provides guidance on notification to the complainant of the IPT's findings:

"(1) In addition to any statement under section 68(4) of the Act, the Tribunal shall provide information to the complainant in accordance with this rule.

(2) Where they make a determination in favour of the complainant, the Tribunal shall provide him with a summary of that determination including any findings of fact.

...

(4) The duty to provide information under this rule is in all cases subject to the general duty imposed on the Tribunal by rule 6(1).

(5) No information may be provided under this rule whose disclosure would be restricted under rule 6(2) unless the person whose consent would be needed for disclosure under that rule has been given the opportunity to make representations to the Tribunal."

134. Rule 6 requires the IPT to carry out its functions in such a way as to ensure that information is not disclosed that is contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, the economic well-being of the United Kingdom or the continued discharge of the functions of any of the intelligence services. Pursuant to Rule 6, in principle, the IPT is not permitted to disclose: the fact that it has held an oral hearing under Rule 9(4); any information disclosed to it in the course of that hearing or the identity of any witness at that hearing; any information otherwise disclosed to it by any person involved in the authorisation or execution of interception warrants, or any information provided by a Commissioner; and the fact that any information has been disclosed or provided. However, the IPT may disclose such information with the consent of the person required to attend the hearing, the person who disclosed the information, the Commissioner, or the person whose consent was required for disclosure of the information, as the case may be. The IPT may also disclose such information as part of the information provided to the complainant under Rule 13(2), subject to the restrictions contained in Rule 13(4) and (5).

135. In *R(A) v. Director of Establishments of the Security Service* [2009] EWCA Civ 24 Lord Justice Laws observed that the IPT was "a judicial body of like standing and authority to the High Court". More recently, in *R(Privacy International) v. Investigatory Powers Tribunal* (cited above) Lord Justice Sales noted that "[t]he quality of the membership of the IPT in terms of judicial expertise and independence is very high".

3. IPT ruling on preliminary issues of law

136. On 23 January 2003, in a case involving a complaint by British-Irish Rights Watch, the IPT gave a ruling on preliminary issues of law, in which it considered whether a number of aspects of its procedure were within the powers conferred on the Secretary of State and Convention compliant. The IPT sat, for the first time, in public.

137. Specifically on the applicability of Article 6 § 1 to the proceedings before it, the IPT found:

> "85. The conclusion of the Tribunal is that Article 6 applies to a person's claims under section 65(2)(a) and to his complaints under section 65(2)(b) of RIPA, as each of them involves 'the determination of his civil rights' by the Tribunal within the meaning of Article 6(1)."

138. The IPT considered that Rule 9 made it clear that oral hearings could be held at its discretion. If a hearing was held, it had to be held in accordance with Rule 9. The absence from the Rules of an absolute right to either an *inter partes* oral hearing, or, failing that, to a separate oral hearing in every case was within the rule-making power in section 69(1) of RIPA and was compatible with the Convention rights under Article 6, 8 and 10. The IPT explained that oral hearings involving evidence or a consideration of the substantive merits of a claim or complaint ran the risk of breaching the "neither confirm nor deny" policy or other aspects of national security and the public interest. It was therefore necessary to provide safeguards against that and the conferring of a discretion to decide when there should be oral hearings and what form they should take was a proportionate response to the need for safeguards.

139. The IPT found the language in Rule 9(6), which stipulates that oral hearings must be held in private, to be clear and unqualified; it therefore had no discretion in the matter. It concluded that the width and blanket nature of the rule went beyond what was authorised by section 69 of RIPA and, as a consequence, it found Rule 9(6) to be *ultra vires* section 69 and not binding on it.

140. The IPT also considered the requirements in Rule 6 for the taking of evidence and disclosure. It concluded that these departures from the adversarial model were within the power conferred on the Secretary of State and compatible with Convention rights in Articles 8 and 10, taking account of the exceptions for the public interest and national security in Articles 8(2) and 10(2), and in particular the effective operation of the legitimate policy of "neither confirm nor deny" in relation to the use of investigatory powers. It noted that disclosure of information was not an absolute right where there were competing interests, such as national security considerations.

141. Finally, as regards the absence of reasons following a negative decision, the IPT concluded that section 68(4) and Rule 13 were valid and binding and that the distinction between information given to the successful complainants and that given to unsuccessful complainants (where the "neither confirm nor deny" policy had to be preserved) was necessary and justifiable.

4. Counsel to the Tribunal

142. The IPT may appoint Counsel to the Tribunal to make submissions on behalf of applicants in hearings at which they cannot be represented. In the *Liberty* case, Counsel to the Tribunal described his role as follows:

> "Counsel to the Tribunal performs a different function [from special advocates in closed proceedings conducted before certain tribunals], akin to that of *amicus curiae*. His or her function is to assist the Tribunal in whatever way the Tribunal directs. Sometimes (e.g. in relation to issues on which all parties are represented), the Tribunal will not specify from what perspective submissions are to be made. In these circumstances, counsel will make submissions according to his or her own analysis of the relevant legal or factual issues, seeking to give particular emphasis to points not fully developed by the parties. At other times (in particular where one or more interests are not represented), the Tribunal may invite its counsel to make submissions from a particular perspective (normally the perspective of the party or parties whose interests are not otherwise represented)."

143. This description was accepted and endorsed by the IPT.

E. Oversight

144. Part IV of RIPA provided for the appointment by the Prime Minister of an Interception of Communications Commissioner and an Intelligence Services Commissioner charged with supervising the activities of the intelligence services.

145. The Interception of Communications Commissioner was responsible for keeping under review the interception of communications and the acquisition and disclosure of communications data by intelligence agencies, police forces and other public authorities. He reported to the Prime Minister on a half-yearly basis with respect to the carrying out of his functions. This report was a public document (subject to the non-disclosure of confidential annexes) which was laid before Parliament. In undertaking his review of surveillance practices, the Commissioner and his inspectors had access to all relevant documents, including closed materials, and all those involved in interception activities had a duty to disclose to him any material he required. The obligation on intercepting agencies to keep records ensured that the Commissioner had effective access to details of surveillance activities undertaken.

146. The Intelligence Services Commissioner also provided independent external oversight of the use of the intrusive powers of the intelligence services and parts of the Ministry of Defence. He also submitted annual reports to the Prime Minister, which were laid before Parliament.

147. However, these provisions, insofar as they relate to England, Scotland and Wales, were repealed by the Investigatory Powers Act 2016 (see paragraphs 195-201 below) and in September 2017 the Investigatory Powers Commissioner's Office ("IPCO") took over responsibility for the

oversight of investigatory powers. The IPCO consists of around fifteen Judicial Commissioners, current and recently retired High Court, Court of Appeal and Supreme Court Judges; a Technical Advisory Panel made up of scientific experts; and almost fifty official staff, including inspectors, lawyers and communications experts. The more intrusive powers such as interception, equipment interference and the use of surveillance in sensitive environments will be subject to the prior approval of a Judicial Commissioner once the provisions of the 2016 Act have entered into force. Use of these and other surveillance powers, including the acquisition of communications data and the use of covert human intelligence sources, are also overseen by a programme of retrospective inspection and audit by Judicial Commissioners and IPCO's inspectors.

F. Reviews of interception operations by the intelligence service

1. Intelligence and Security Committee of Parliament: July 2013 Statement on GCHQ's alleged interception of communications under the US PRISM programme

148. The Intelligence and Security Committee of Parliament ("the ISC") was originally established by the Intelligence Services Act 1994 to examine the policy, administration and expenditure of MI5, MI6, and GCHQ. Since the introduction of the Justice and Security Act 2013, however, the ISC was expressly given the status of a Committee of Parliament; was provided with greater powers; and its remit was increased to include *inter alia* oversight of operational activity and the wider intelligence and security activities of Government. Pursuant to sections 1-4 of the Justice and Security Act 2013, it consists of nine members drawn from both Houses of Parliament, and, in the exercise of their functions, those members are routinely given access to highly classified material in carrying out their duties.

149. Following the Edward Snowden revelations, the ISC conducted an investigation into GCHQ's access to the content of communications intercepted under the US PRISM programme, the legal framework governing access, and the arrangements GCHQ had with its overseas counterpart for sharing information. In the course of the investigation, the ISC took detailed evidence from GCHQ and discussed the programme with the NSA.

150. The ISC concluded that allegations that GCHQ had circumvented United Kingdom law by using the NSA PRISM programme to access the content of private communications were unfounded as GCHQ had complied with its statutory duties contained in the ISA. It further found that in each case where GCHQ sought information from the United States, a warrant for interception, signed by a Government Minister, had already been in place. However, it found it necessary to further consider whether the current

statutory framework governing access to private communications remained accurate.

2. Privacy and security: a modern and transparent legal framework

151. Following its statement in July 2013, the ISC conducted a more in-depth inquiry into the full range of the intelligence services' capabilities. Its report, which contained an unprecedented amount of information about the intelligence services' intrusive capabilities, was published on 12 March 2015 (see paragraphs 11-13 above).

152. The ISC was satisfied that the United Kingdom's intelligence and security services did not seek to circumvent the law, including the requirements of the Human Rights Act 1998, which governs everything that they do. However, it considered that as the legal framework had developed piecemeal, it was unnecessarily complicated. The ISC therefore had serious concerns about the resulting lack of transparency, which was not in the public interest. Consequently, its key recommendation was that the current legal framework be replaced by a new Act of Parliament which should clearly set out the intrusive powers available to the intelligence services, the purposes for which they may use them, and the authorisation required before they may do so.

153. With regard to GCHQ's bulk interception capability, the inquiry showed that the intelligence services did not have the legal authority, the resources, the technical capability, or the desire to intercept every communication of British citizens, or of the Internet as a whole: thus, GCHQ were not reading the emails of everyone in the United Kingdom. On the contrary, GCHQ's bulk interception systems operated on a very small percentage of the bearers that made up the Internet and the ISC was satisfied that GCHQ applied levels of filtering and selection such that only a certain amount of the material on those bearers was collected. Further targeted searches ensured that only those items believed to be of the highest intelligence value were ever presented for analysts to examine, and therefore only a tiny fraction of those collected were ever seen by human eyes.

154. In respect of Internet communications, the ISC considered that the current system of 'internal' and 'external' communications was confusing and lacked transparency and it therefore suggested that the Government publish an explanation of which Internet communications fall under which category, including a clear and comprehensive list of communications.

155. Nevertheless, the inquiry had established that bulk interception could not be used to target the communications of an individual in the United Kingdom without a specific authorisation naming that individual, signed by a Secretary of State.

156. With regard to section 8(4) warrants, the ISC observed that the warrant itself was very brief. It further noted that insofar as the

accompanying certificate set out the categories of communications which might be examined, those categories were expressed in very general terms (for example, "material providing intelligence on terrorism (as defined by the Terrorism Act 2000 (as amended)), including, but not limited to, terrorist organisations, terrorists, active sympathisers, attack planning, fund-raising"). Given that the certificate was so generic, the ISC questioned whether it needed to be secret or whether, in the interests of transparency, it could be published.

157. Although the section 8(4) certificate set out the general categories of information which might be examined, the ISC observed that in practice, it was the selection of the bearers, the application of simple selectors and initial search criteria, and then complex searches which determined what communications were examined. The ISC had therefore sought assurances that these were subject to scrutiny and review by Ministers and/or the Commissioners. However, the evidence before the ISC indicated that neither Ministers nor the Commissioners had any significant visibility of these issues. The ISC therefore recommended that the Interception of Communications Commissioner should be given statutory responsibility to review the various selection criteria used in bulk interception to ensure that they followed directly from the Certificate and valid national security requirements.

158. The ISC noted that communications data was central to most intelligence services' investigations: it could be analysed to find patterns that reflected particular online behaviours associated with activities such as attack planning, and to establish links, to help focus on individuals who might pose a threat, to ensure that interception was properly targeted, and to illuminate networks and associations relatively quickly. It was particularly useful in the early stages of an investigation, when the intelligence services had to be able to determine whether those associating with a target were connected to the plot (and therefore required further investigation) or were innocent bystanders. According to the Secretary of State for the Home Department, it had "played a significant role in every Security Service counter-terrorism operation over the last decade". Nevertheless, the ISC expressed concern about the definition of "communications data". While it accepted that there was a category of communications data which was less intrusive than content, and therefore did not require the same degree of protection, it considered that there now existed certain categories of communications data which had the potential to reveal more intrusive details about a person's private life and, therefore, required greater safeguards.

159. Finally, with regard to the IPT, it expressly recognised the importance of a domestic right of appeal.

3. "A Question of Trust": Report of the Investigatory Powers Review by the Independent Reviewer of Terrorism Legislation ("the Anderson Report")

160. The Independent Reviewer of Terrorism Legislation, a role that has existed since the late 1970s, is an independent person, appointed by the Home Secretary and by the Treasury for a renewable three-year term and tasked with reporting to the Home Secretary and to Parliament on the operation of counter-terrorism law in the United Kingdom. These reports are then laid before Parliament, to inform the public and political debate. The Independent Reviewer's role is to inform the public and political debate on anti-terrorism law in the United Kingdom. The uniqueness of the role lies in its complete independence from government, coupled with access based on a very high degree of clearance to secret and sensitive national security information and personnel.

161. The purpose of the Anderson Report, published in June 2015 and identified by reference to the then Independent Reviewer of Terrorism Legislation, was to inform the public and political debate on the threats to the United Kingdom, the capabilities required to combat those threats, the safeguards in place to protect privacy, the challenges of changing technology, issues relating to transparency and oversight, and the case for new or amended legislation. In conducting the review the Independent Reviewer had unrestricted access, at the highest level of security clearance, to the responsible Government departments and public authorities. He also engaged with service providers, independent technical experts, non-governmental organisations, academics, lawyers, judges and regulators.

162. The Independent Reviewer noted that the statutory framework governing investigatory powers had developed in a piecemeal fashion, with the consequence that there were "few [laws] more impenetrable than RIPA and its satellites".

163. With regard to the importance of communications data, he observed that it enabled the intelligence services to build a picture of a subject of interest's activities and was extremely important in providing information about criminal and terrorist activity. It identified targets for further work and also helped to determine if someone was completely innocent. Of central importance was the ability to use communications data (subject to necessity and proportionality) for:

(a) linking an individual to an account or action (for example, visiting a website, sending an email) through IP resolution;

(b) establishing a person's whereabouts, traditionally via cell site or GPRS data;

(c) establishing how suspects or victims are communicating (that is, via which applications or services);

(d) observing online criminality (for example, which websites are being visited for the purposes of terrorism, child sexual exploitation or purchases of firearms or illegal drugs); and

(e) exploiting data (for example, to identify where, when and with whom or what someone was communicating, how malware or a denial of service attack was delivered, and to corroborate other evidence).

164. Moreover, analysis of communications data could be performed speedily, making it extremely useful in fast-moving operations, and use of communications data could build a case for using a more intrusive measure, or deliver the information that would make other measures unnecessary.

165. His proposals for reform can be summarised as follows:

(a) A comprehensive and comprehensible new law should be drafted, replacing "the multitude of current powers" and providing clear limits and safeguards on any intrusive power it may be necessary for public authorities to use;

(b) The definitions of "content" and "communications data" should be reviewed, clarified and brought up-to-date;

(c) The capability of the security and intelligence agencies to practice bulk collection of intercepted material and associated communications data should be retained, but only subject to strict additional safeguards including the authorisation of all warrants by a Judicial Commissioner at a new Independent Surveillance and Intelligence Commission ("ISIC");

(d) The purposes for which material or data was sought should be spelled out in the accompanying certificate by reference to specific operations or mission purposes (for example, "attack planning by ISIL in Iraq/Syria against the UK");

(e) There should be a new form of bulk warrant limited to the acquisition of communications data which could be a proportionate option in certain cases;

(f) Regarding the authorisation for the acquisition of communications data, designated persons should be required by statute to be independent from the operations and investigations in relation to which the authorisation is sought;

(g) Novel or contentious requests for communications data, or requests for the purpose of determining matters that are privileged or confidential, should be referred to the ISIC for determination by a Judicial Commissioner;

(h) The ISIC should take over intelligence oversight functions and should be public-facing, transparent and accessible to the media; and

(i) The IPT should have the capacity to make declarations of incompatibility and its rulings should be subject to appeals on points of law.

4. A Democratic Licence to Operate: Report of the Independent Surveillance Review ("ISR")

166. The ISR was undertaken by the Royal United Services Institute, an independent think-tank, at the request of the then deputy Prime Minister, partly in response to the revelations by Edward Snowden. Its terms of reference were to look at the legality of United Kingdom surveillance programmes and the effectiveness of the regimes that govern them, and to suggest reforms which might be necessary to protect both individual privacy and the necessary capabilities of the police and security and intelligence services.

167. Despite the revelations by Edward Snowden, having completed its review the ISR found no evidence that the British Government was knowingly acting illegally in intercepting private communications, or that the ability to collect data in bulk was being used by the Government to provide it with a perpetual window into the private lives of British citizens. On the other hand, it found evidence that the present legal framework authorising the interception of communications was unclear, had not kept pace with developments in communications' technology, and did not serve either the Government or members of the public satisfactorily. It therefore concluded that a new, comprehensive and clearer legal framework was required.

168. In particular, it supported the view set out in both the ISC and Anderson reports that while the current surveillance powers were needed, both a new legislative framework and oversight regime were required. It further considered that the definitions of "content" and "communications data" should be reviewed as part of the drafting of the new legislation so that they could be clearly delineated in law.

169. With regard to communications data, the report noted that greater volumes were available on an individual relative to content, since every piece of content was surrounded by multiple pieces of communications data. Furthermore, aggregating data sets could create an extremely accurate picture of an individual's life since, given enough raw data, algorithms and powerful computers could generate a substantial picture of the individual and his or her patterns of behaviour without ever accessing content. In addition, the use of increasingly sophisticated encryption methods had made content increasingly difficult to access.

170. It further considered that the capability of the security and intelligence services to collect and analyse intercepted material in bulk should be maintained, but with the stronger safeguards recommended in the Anderson Report. In particular, it agreed that warrants for bulk interception should include much more detail than is currently the case and should be the subject of a judicial authorisation process, save for when there is an urgent requirement.

171. In addition, it agreed with both the ISC and the Anderson report that there should be different types of warrant for the interception and acquisition of communications and related data. It was proposed that warrants for a purpose relating to the detection or prevention of serious and authorised crime should always be authorised by a Judicial Commissioner, while warrants for purposes relating to national security should be authorised by the Secretary of State subject to judicial review by a Judicial Commissioner.

172. With regard to the IPT, the ISR recommended open public hearings, except where it was satisfied private or closed hearings were necessary in the interests of justice or other identifiable public interest. Furthermore, it should have the ability to test secret evidence put before it, possibly through the appointment of Special Counsel. Finally, it agreed with the ISC and Anderson reports that a domestic right of appeal was important and should be considered in future legislation.

5. Report of the Bulk Powers Review

173. The bulk powers review was set up in May 2016 to evaluate the operational case for the four bulk powers contained in what was then the Investigatory Powers Bill (now the Investigatory Powers Act 2016: see paragraphs 195-201 below). Those powers related to bulk interception and the bulk acquisition of communications data, bulk equipment interference and the acquisition of bulk personal datasets.

174. The review was again carried out by the Independent Reviewer of Terrorism Legislation. To conduct the review he recruited three team members, all of whom had the necessary security clearance to access very highly classified material, including a person with the necessary technical background to understand the systems and techniques used by GCHQ, and the uses to which they could be put; an investigator with experience as a user of secret intelligence, including intelligence generated by GCHQ; and senior independent counsel with the skills and experience to challenge forensically the evidence and the case studies presented by the security and intelligence services.

175. In conducting their review, the team had significant and detailed contact with the intelligence services at all levels of seniority as well as the relevant oversight bodies (including the IPT and Counsel to the Tribunal in the relevant cases), NGOs and independent technical experts.

176. Although the review was of the Investigatory Powers Bill, a number of its findings in respect of bulk interception are relevant to the case at hand. In particular, having examined a great deal of closed material, the review concluded that it was an essential capability: first, because terrorists, criminal and hostile foreign intelligence services had become increasingly sophisticated at evading detection by traditional means; and secondly, because the nature of the global Internet meant that the route a particular

communication would travel had become hugely unpredictable. The review team looked at alternatives to bulk interception (including targeted interception, the use of human sources and commercial cyber-defence products) but concluded that no alternative or combination of alternatives would be sufficient to substitute for the bulk interception power as a method of obtaining the necessary intelligence.

6. Attacks in London and Manchester March-June 2017: Independent Assessment of MI5 and Police Internal Reviews

177. Following a series of four terrorist attacks in the short period between March and June 2017, in the course of which some 36 innocent people were killed and almost 200 more were injured, the Home Secretary asked the recently retired Independent Reviewer of Terrorism Legislation, David Anderson Q.C. to assess the classified internal reviews of the police and intelligence services involved. In placing the attacks in context, the Report made the following observations:

> "1.2 The attacks under review were the most deadly terrorist attacks on British soil since the 7/7 London tube and bus bombings of July 2005. All four were shocking for their savagery and callousness. The impact of the first three attacks was increased by the fact that they came at the end of a long period in which Islamist terrorism had taken multiple lives in neighbouring countries such as France, Belgium and Germany but had not enjoyed equivalent success in Britain.
>
> 1.3 The plots were part of an increasingly familiar pattern of Islamist and (to a lesser extent) anti-Muslim terrorist attacks in western countries, including in particular northern Europe. The following points provide context, and an indication that lessons learned from these incidents are likely to be transferrable.
>
> 1.4 First, the ***threat level*** in the UK from so-called "international terrorism" (in practice, Islamist terrorism whether generated at home or abroad) has been assessed by the Joint Terrorism Analysis Centre (JTAC) as SEVERE since August 2014, indicating that Islamist terrorist attacks in the UK are "highly likely". Commentators with access to the relevant intelligence have always been clear that this assessment is realistic. They have pointed also to the smaller but still deadly threat from extreme right wing (XRW) terrorism, exemplified by the murder of Jo Cox MP in June 2016 and by the proscription of the neo-Nazi group National Action in December 2016.
>
> 1.5 Secondly, the ***growing scale*** of the threat from Islamist terrorism is striking. The Director General of MI5, Andrew Parker, spoke in October 2017 of "a dramatic upshift in the threat this year" to "the highest tempo I've seen in my 34 year career". Though deaths from Islamist terrorism occur overwhelmingly in Africa, the Middle East and South Asia, the threat has grown recently across the western world, and has been described as "especially diffuse and diverse in the UK". It remains to be seen how this trend will be affected, for good or ill, by the physical collapse of the so-called Islamic State in Syria and Iraq.
>
> 1.6 Thirdly, the profiles of the ***attackers*** ... display many familiar features. Comparing the five perpetrators of the Westminster, Manchester and London Bridge attacks with those responsible for the 269 Islamist-related terrorist offences in the UK between 1998-2015, as analysed by Hannah Stuart ("the total"):

(a) All were ***male***, like 93% of the total.

(b) Three were ***British*** (Masood, Abedi, Butt), like 72% of the total.

(c) One was a ***convert to Islam*** (Masood), like 16% of the total.

(d) Three ***resided*** in London (43% of the total) and one in North West England (10% of the total).

(e) Three (Masood, and to a more limited extent Abedi and Butt) were ***known to the police***, like 38% of the total.

(f) The same three were ***known to MI5***, like 48% of the total.

(g) At least one (Butt) had direct links to a ***proscribed terrorist organisation***, as had 44% of the total. His links, in common with 56% of the total who had links with such organisations, were with ***Al-Muhajiroun*** (ALM).

In view of their possible pending trials I say nothing of Hashem Abedi, currently detained in Libya in connection with the Manchester attack, or of the Finsbury Park attacker Darren Osborne who (like Khalid Masood at Westminster) is not alleged to have had accomplices.

1.7 Fourthly, though the ***targets*** of the first three attacks did not extend to the whole of the current range, they had strong similarities to the targets of other recent western attacks: political centres (e.g. Oslo 2011, Ottawa 2014, Brussels 2016); concert-goers, revellers and crowds (e.g. Orlando 2016, Paris 2016, Barcelona 2017); and police officers (e.g. Melbourne 2014, Berlin 2015, Charleroi 2016). There are precedents also for attacks on observant Muslims which have crossed the boundary from hate crime to terrorism, including the killing of Mohammed Saleem in the West Midlands in 2013.

1.8 Fifthly, the ***modus operandi*** (MO) of terrorist attacks has diversified and simplified over the years, as Daesh has employed its formidable propaganda effort to inspire rather than to direct acts of terrorism in the west. The attacks under review were typical in style for their time and place:

(a) Unlike the large, directed Islamist plots characteristic of the last decade, all four attacks were committed by ***lone actors*** or ***small groups***, with little evidence of detailed planning or precise targeting.

(b) Strong gun controls in the UK mean that ***bladed weapons*** are more commonly used than firearms in gang-related and terrorist crime.

(c) Since a truck killed 86 innocent people in Nice (July 2016), ***vehicles*** – which featured in three of the four attacks under review – have been increasingly used as weapons.

(d) The ***combination*** of a vehicle and bladed weapons, seen at Westminster and London Bridge, had previously been used to kill the soldier Lee Rigby (Woolwich, 2013).

(e) ***Explosives***, used in Manchester, were the most popular weapon for Islamist terrorists targeting Europe between 2014 and 2017. The explosive TATP has proved to be capable of manufacture (aided by on-line purchases and assembly instructions) more easily than was once assumed."

7. Annual Report of the Interception of Communications Commissioner for 2016

(a) Section 8(4) warrants

178. The Commissioner observed that when conducting interception under a section 8(4) warrant, an intercepting agency had to use its knowledge of the way in which international communications were routed, combined with regular surveys of relevant communications links, to identify those individual communications bearers that were most likely to contain external communications that would meet the descriptions of material certified by the Secretary of State under section 8(4). It also had to conduct the interception in ways that limited the collection of non-external communications to the minimum level compatible with the objective of intercepting the wanted external communications.

179. He further observed that prior to analysts being able to read, look at or listen to material, they had to provide a justification, which included why access to the material was required, consistent with, and pursuant to section 16 and the applicable certificate, and why such access was proportionate. Inspections and audits showed that although the selection procedure was carefully and conscientiously undertaken, it relied on the professional judgment of analysts, their training and management oversight.

180. According to the report, 3007 interception warrants were issued in 2016 and five applications were refused by a Secretary of State. In the view of the Commissioner, these figures did not capture the critical quality assurance function initially carried out by the staff and lawyers within the intercepting agency or the warrant-granting department (the warrant-granting departments were a source of independent advice to the Secretary of State and performed pre-authorisation scrutiny of warrant applications and renewals to ensure that they were (and remained) necessary and proportionate). Based on his inspections, he was confident that the low number of rejections reflected the careful consideration given to the use of these powers.

181. A typical inspection of an interception agency included the following:

- a review of the action points or recommendations from the previous inspection and their implementation;
- an evaluation of the systems in place for the interception of communications to ensure they were sufficient for the purposes of Chapter 1 of Part 1 of RIPA and that all relevant records had been kept;
- the examination of selected interception applications to assess whether they were necessary in the first instance and then whether the requests met the necessity and proportionality requirements;

- interviews with case officers, analysts and/or linguists from selected investigations or operations to assess whether the interception and the justifications for acquiring all of the material were proportionate;
- the examination of any urgent oral approvals to check that the process was justified and used appropriately;
- a review of those cases where communications subject to legal privilege or otherwise confidential information had been intercepted and retained, and any cases where a lawyer was the subject of an investigation;
- a review of the adequacy of the safeguards and arrangements under sections 15 and 16 of RIPA;
- an investigation of the procedures in place for the retention, storage and destruction of intercepted material and related communications data; and
- a review of the errors reported, including checking that the measures put in place to prevent recurrence were sufficient.

182. After each inspection, inspectors produced a report, including:

- an assessment of how far the recommendations from the previous inspection had been achieved;
- a summary of the number and type of interception documents selected for inspection, including a detailed list of those warrants;
- detailed comments on all warrants selected for further examination and discussion during the inspection;
- an assessment of the errors reported to the Commissioner's office during the inspection period;
- an account of the examination of the retention, storage and destruction procedures;
- an account of other policy or operational issues which the agency or warrant-granting departments raised during the inspection;
- an assessment of how any material subject to legal professional privilege (or otherwise confidential material) has been handled;
- a number of recommendations aimed at improving compliance and performance.

183. During 2016, the Commissioner's office inspected all nine interception agencies once and the four main warrant-granting departments twice. This, together with extra visits to GCHQ, made a total of twenty-two inspection visits. In addition, he and his inspectors arranged other *ad hoc* visits to agencies.

184. Inspection of the systems in place for applying for and authorising interception warrants usually involved a three-stage process. First, to achieve a representative sample of warrants, inspectors selected them across different crime types and national security threats. In addition, inspectors

focussed on those of particular interest or sensitivity (such as those which gave rise to an unusual degree of collateral intrusion, those which have been extant for a considerable period, those which were approved orally, those which resulted in the interception of legal or otherwise confidential communications, and so-called 'thematic' warrants). Secondly, inspectors scrutinised the selected warrants and associated documentation in detail during reading days which preceded the inspections. Thirdly, they identified those warrants, operations or areas of the process which required further information or clarification and arranged to interview relevant operational, legal or technical staff. Where necessary, they examined further documentation or systems relating to those warrants.

185. 970 warrants were examined during the twenty-two interception inspections (sixty-one percent of the number of warrants in force at the end of the year and thirty-two percent of the total of new warrants issued in 2016).

186. According to the report, every interception agency had a different view on what constituted an appropriate retention period for intercepted material and related communications data. There was no period prescribed by the legislation, but the agencies had to consider section 15(3) of RIPA, which provided that the material or data had to be destroyed as soon as retaining it was no longer necessary for any of the authorised purposes in section 15(4). The vast majority of content was reviewed and automatically deleted after a very short period of time unless specific action was taken to retain the content for longer because it was necessary to do so. The retention periods differed within the interception agencies and ranged between thirty days and one year. The retention periods for related communications data also differed within the interception agencies, but ranged between six months and one year.

187. Inspectors made a total of twenty-eight recommendations in their inspection reports, eighteen of which were made in relation to the application process. The majority of the recommendations in this category related to the necessity, proportionality and/or collateral intrusion justifications in the applications; or the handling of legally privileged or otherwise confidential material relating to sensitive professions.

188. The total number of interception errors reported to the Commissioner during 2016 was 108. Key causes of interception errors were over-collection (generally technical software or hardware errors that caused over-collection of intercepted material and related communications data), unauthorised selection/examination, incorrect dissemination, the failure to cancel interception, and the interception of either an incorrect communications address or person.

(b) Acquisition of communications data under Chapter II of RIPA

189. According to the report, police forces and law enforcement agencies were responsible for acquiring ninety-three percent of the total number of items of data in 2016, six percent was acquired by intelligence services and the remaining one percent was acquired by other public authorities, including local authorities. Fifty percent of the data acquired was subscriber information, forty-eight percent was traffic data and two percent service use information. Most of the acquired items of data (eighty-one percent) related to telephony, such as landlines or mobile phones. Internet identifiers, for example email or IP addresses, accounted for fifteen percent of the acquired data and two percent of requests were related to postal identifiers.

190. With regard to the purpose of the request, eighty-three percent of the items of data were acquired for the purpose of preventing or detecting crime or preventing disorder; eleven percent were acquired for the purpose of preventing death or injury or damage to a person's mental health, or of mitigating any injury or damage to a person's physical or mental health; and six percent were acquired in the interests of national security.

191. Furthermore, approximately seventy percent of data requests were for data less than three months old, twenty-five percent aged between three months and one year, and six percent for data over twelve months old. Eighty-one percent of the requests required data for a communications address for periods of three months or less (for example, three months of incoming and outgoing call data for a communications address). Twenty-five percent of all requests were for data relating to a period of less than one day.

192. Twenty-seven percent of submitted applications were returned to the applicant by the Single Point of Contact ("SPoC") for development and a further five percent were declined by the SPoC. Reasons for refusing data applications included: lack of clarity; failure to link the crime to the communications address; and insufficient justification for collateral intrusion. Four percent of submitted applications were returned to applicants by designated persons for further development and one percent was rejected. The main reason for designated persons returning or rejecting applications was that they were not satisfied with the necessity or proportionality justifications given (fifty-two percent). A significant number of applications were returned because designated persons were not satisfied with the overall quality or clarity of the application (twenty-one percent). Other reasons for rejection included the designated persons declaring that they were not independent of the investigation and requesting that the application be forwarded to an independent designated person for consideration (six percent).

193. In 2016 forty-seven public authorities advised that they had made a total of 948 applications that related to persons who were members of

sensitive professions. A significant proportion of these 948 applications were categorised incorrectly (that is, the applicant had recorded a sensitive profession when there was not one). This was usually because the applicant erred on the side of caution, recording a sensitive profession if there was a possibility of one, rather than because they knew that there was one, a fact which provided the Commissioner with "a greater level of assurance that [designated persons] are taking sensitive professions into account when necessary". Furthermore, according to the Commissioner, most applications relating to members of sensitive professions were submitted because the individual had been a victim of crime or was the suspect in a criminal investigation. In these cases, the profession of the individual was usually not relevant to the investigation, but public authorities showed proper consideration of the sensitive profession by bringing it to the attention of the authorising officer.

194. Having considered the "reportable errors", the Commissioner noted that the number of serious errors remained very low (0.004%).

G. The Investigatory Powers Act 2016

195. The Investigatory Powers Act 2016 received Royal Assent on 29 November 2016.

196. On 30 December 2016 Part 4 of the 2016 Act, which included a power to issue "retention notices" to telecommunications operators requiring the retention of data, came into force (although not in its entirety). Following a legal challenge by Liberty, the Government conceded that Part 4 of the IPA was, in its current form, inconsistent with the requirements of EU law. Part 4 was not amended and on 27 April 2018 the High Court found Part 4 to be incompatible with fundamental rights in EU law since, in the area of criminal justice, access to retained data was not limited to the purpose of combating "serious crime"; and access to retained data was not subject to prior review by a court or an independent administrative body. The court concluded that the legislation had to be amended by 1 November 2018.

197. On 13 February 2017 the provisions of the IPA relating to the appointment of the Investigatory Powers Commissioner and other Judicial Commissioners came into force. On 3 March 2017, the Government appointed the first Investigatory Powers Commissioner (a judge currently sitting on the Court of Appeal and former justice of the International Criminal Court) for a three-year term and he took up appointment with immediate effect. The newly created Investigatory Powers Commissioners Office ("ICPO") commenced operations on 8 September 2017 and is ultimately due to consist of around 70 staff (including approximately fifteen judicial commissioners made up of current and recently retired judges of the

High Court, Court of Appeal and Supreme Court, and a technical advisory panel of scientific experts).

198. The remainder of the 2016 Act is not yet in force.

199. In terms of safeguards, when it enters into force in full the Act will require that bulk interception and bulk equipment interference warrants may only be issued where the main purpose of the interception is to acquire intelligence relating to individuals outside the United Kingdom, even where the conduct occurs within the United Kingdom. Similarly, interference with the privacy of persons in the United Kingdom will be permitted only to the extent that it is necessary for that purpose. It will also introduce a "double-lock" for the most intrusive surveillance powers, meaning that a warrant issued by the Secretary of State will also require the approval of one of the appointed Judicial Commissioners. There will also be new protections for journalistic and legally privileged material, including a requirement for judicial authorisation for the acquisition of communications data identifying journalists' sources; tough sanctions for the misuse of powers, including the creation of new criminal offences; and a right of appeal from the IPT.

200. In addition, the new Act will consolidate and update the powers available to the State to obtain communications and communications data. It will provide an updated framework for the use (by the security and intelligence services, law enforcement and other public authorities) of investigatory powers to obtain communications and communications data. These powers cover the interception of communications, the retention and acquisition of communications data, and equipment interference for obtaining communications and other data. The Act also makes provision relating to the security and intelligence services' retention and examination of bulk personal datasets.

201. On 23 February 2017 the Home Office launched a public consultation on the five draft codes of practice it intends to issue under the 2016 Act (on the Interception of Communications, Equipment Interference, Bulk Communications Data Acquisition, Retention and Use of Bulk Personal Datasets by the Security and Intelligence Agencies and National Security Notices), which will set out the processes and safeguards governing the use of investigatory powers by public authorities. They will give detail on how the relevant powers should be used, including examples of best practice. They are intended to provide additional clarity and to ensure the highest standards of professionalism and compliance with the relevant legislation. Following the closure of the consultation on 6 April 2017, the draft codes were further amended and Regulations bringing them into force will be laid and debated before Parliament. They will only come into force when they have been debated in both Houses of Parliament and approved by a resolution in both Houses.

H. Relevant international law

1. The United Nations

(a) Resolution no. 68/167 on The Right to Privacy in the Digital Age

202. Resolution no. 68/167, adopted by the General Assembly on 18 December 2013, reads as follows:

> "The General Assembly,
>
> ...
>
> 4. *Calls upon* all States:
>
> ...
>
> (*c*) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;
>
> (*d*) To establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data ..."

(b) The Constitution of the International Telecommunication Union 1992

203. Articles 33 and 37 of the Constitution provide as follows:

The Right of the Public to Use the International Telecommunication Service

"Member States recognize the right of the public to correspond by means of the international service of public correspondence. The services, the charges and the safeguards shall be the same for all users in each category of correspondence without any priority or preference.
..."

Secrecy of Telecommunications

> "1. Member States agree to take all possible measures, compatible with the system of telecommunication used, with a view to ensuring the secrecy of international correspondence.

2. Nevertheless, they reserve the right to communicate such correspondence to the competent authorities in order to ensure the application of their national laws or the execution of international conventions to which they are parties."

(c) The 2006 Annual Report of the International Law Commission

204. In its 2006 Annual Report the ILC proposed to include the topic "Protection of personal data in the transborder flow of information" in its

long-term programme of work. The Secretariat's supporting report (Annex D) identifies a number of core principles of public international law:

Core principles

"23. A number of core principles are discernible from developments in this field in almost forty-years. Such principles include the following:

Lawful and fair data collection and processing: This principle presupposes that the collection of personal data would be restricted to a necessary minimum. In particular such data should not be obtained unlawfully or through unfair means;

Accuracy: The information quality principle is a qualitative requirement and entails a responsibility that the data be accurate, and necessarily complete and up to date for the purpose intended.

Purpose specification and limitation: This principle establishes the requirement that the purpose for which the data are collected should be specified to the data subject. Data should not be disclosed, made available or otherwise used for purposes other than those specified. It has to be done with the consent or knowledge of the data-subject or under the operation of the law. Any subsequent use is limited to such purpose, or any other that is not incompatible with such purpose. Differences lie in the approaches taken by States. Some jurisdictions perceive the obligation for consent to be ex ante.

Proportionality: Proportionality requires that the necessary measure taken should be proportionate to the legitimate claims being pursued.

Transparency: Denotes a general policy of openness regarding developments, practices and policies with respect to protection of personal data.

Individual participation and in particular the right to access: This principle may be the most important for purposes of data protection. The individual should have access to such data; as well as to the possibility of determining whether or not the keeper of the file has data concerning him; to obtain such information or to have it communicated to him in a form, in a manner and at a cost that is reasonable. This accords with the right of an individual to know about the existence of any data file, its contents, to challenge the data and to have it corrected, amended or erased.

Non-discrimination: This principle connotes that data likely to give rise to unlawful and arbitrary discrimination should not be compiled. This includes information collated on racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union.

Responsibility: This principle embraces data security; data should be protected by reasonable and appropriate measures to prevent their loss, destruction, unauthorized access, use, modification or disclosure and the keeper of the file should be accountable for it.

Independent supervision and legal sanction: Supervision and sanction require that there should be a mechanism for ensuring due process and accountability. There should be an authority accountable in law for giving effect to the requirements of data protection.

Data equivalency in the case of transborder flow of personal data: This is a principle of compatibility; it is intended to avoid the creation of unjustified obstacles and restrictions to the free flow of data, as long as the circulation is consistent with the standard or deemed adequate for that purpose.

The principle of derogability: This entails power to make exceptions and impose limitations if they are necessary to protect national security, public order, public health or morality or to protect the rights of others."

Derogability

"24. While privacy concerns are of critical importance, such concerns have to be balanced with other value-interests. The privacy values to avoid embarrassment, to

construct intimacy and to protect against misuse associated with the need to protect the individual have to be weighed against other counter-values against individual control over personal information; such as the need not to disrupt the flow of international trade and commerce and the flow of information; the importance of securing the truth, as well as the need to be live in secure environment. There are allowable restrictions and exceptions, for example, with respect to national security, public order (ordre public), public health or morality or in order to protect the rights and freedoms of others, as well as the need for effective law enforcement and judicial cooperation in combating crimes at the international level, including the threats posed by international terrorism and organized crime.

25. The processing of personal data must be interpreted in accordance with human rights principles. Accordingly, any of the objectives in the public interest would justify interference with private life if it is (a) in accordance with the law, (b) is necessary in a democratic society for the pursuit of legitimate aims, and (c) is not disproportionate to the objective pursued. The phrase "in accordance with the law" goes beyond to the formalism of having in existence a legal basis in domestic law, it requires that the legal basis be "accessible" and foreseeable". Foreseeability necessitates sufficiency of precision in formulation of the rule to enable any individual to regulate his conduct."

2. The Council of Europe

(a) The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981

205. The Convention, which entered into force in respect of the United Kingdom on 1 December 1987, sets out standards for data protection in the sphere of automatic processing of personal data in the public and private sectors. It provides, insofar as relevant:

Preamble

"The member States of the Council of Europe, signatory hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;

Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing;

Reaffirming at the same time their commitment to freedom of information regardless of frontiers;

Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,

Have agreed as follows:"

Article 1 – Object and purpose

"The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and

fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").

..."

Article 8 – Additional safeguards for the data subject

"Any person shall be enabled:

a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;

d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with."

Article 9 – Exceptions and restrictions

"1. No exception to the provisions of Articles 5, 6 and 8 of this Convention shall be allowed except within the limits defined in this article.

2. Derogation from the provisions of Articles 5, 6 and 8 of this Convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

b. protecting the data subject or the rights and freedoms of others.

..."

Article 10 – Sanctions and remedies

"Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter."

206. The Explanatory Report explains that:

Article 9 – Exceptions and restrictions

"55. Exceptions to the basic principles for data protection are limited to those which are necessary for the protection of fundamental values in a democratic society. The text of the second paragraph of this article has been modelled after that of the second paragraphs of Articles 6, 8, 10 and 11 of the European Human Rights Convention. It is clear from the decisions of the Commission and the Court of Human Rights relating to the concept of "necessary measures" that the criteria for this concept cannot be laid down for all countries and all times, but should be considered in the light of the given situation in each country.

56. Littera a in paragraph 2 lists the major interests of the State which may require exceptions. These exceptions are very specific in order to avoid that, with regard to the general application of the convention, States would have an unduly wide leeway.

States retain, under Article 16, the possibility to refuse application of the convention in individual cases for important reasons, which include those enumerated in Article 9.

The notion of "State security" should be understood in the traditional sense of protecting national sovereignty against internal or external threats, including the protection of the international relations of the State."

(b) The Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows of 8 November 2001 (CETS No. 181)

207. The Protocol, which has not been ratified by the United Kingdom, provides, insofar as relevant:

Article 1 – Supervisory authorities

"1. Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention and in this Protocol.

2. a. To this end, the said authorities shall have, in particular, powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the principles mentioned in paragraph 1 of Article 1 of this Protocol.

b. Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence.

3. The supervisory authorities shall exercise their functions in complete independence.

4. Decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts.

..."

Article 2 – Transborder flows of personal data to a recipient which is not subject to the jurisdiction of a Party to the Convention

"1. Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer.

2. By way of derogation from paragraph 1 of Article 2 of this Protocol, each Party may allow for the transfer of personal data:

a. if domestic law provides for it because of:

– specific interests of the data subject, or

– legitimate prevailing interests, especially important public interests, or

b. if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law."

(c) Recommendation of the Committee of Ministers on the protection of personal data in the area of telecommunication services

208. This Recommendation (No. R (95) 4 of the Committee of Ministers), which was adopted on 7 February 1995, reads, insofar as relevant, as follows:

"2.4. Interference by public authorities with the content of a communication, including the use of listening or tapping devices or other means of surveillance or interception of communications, must be carried out only when this is provided for by law and constitutes a necessary measure in a democratic society in the interests of:

a. protecting state security, public safety, the monetary interests of the state or the suppression of criminal offences;

b. protecting the data subject or the rights and freedoms of others.

2.5. In the case of interference by public authorities with the content of a communication, domestic law should regulate:

a. the exercise of the data subject's rights of access and rectification;

b. in what circumstances the responsible public authorities are entitled to refuse to provide information to the person concerned, or delay providing it;

c. storage or destruction of such data.

If a network operator or service provider is instructed by a public authority to effect an interference, the data so collected should be communicated only to the body designated in the authorisation for that interference."

(d) The 2001 (Budapest) Convention on Cybercrime

209. The Convention provides, insofar as relevant:

Preamble

"The member States of the Council of Europe and the other States signatory hereto,

...

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

...

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems."

Article 2 – Illegal access

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."

Article 3 – Illegal interception

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system."

Article 4 – Data interference

"1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

..."

Article 15 – Conditions and safeguards

"1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality."

210. The Explanatory Report explains that:

"38. A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self-defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised. Specific examples of such exceptions from criminalisation are provided in relation to specific offences in the corresponding text of the Explanatory Memorandum below. It is left to the Parties to determine how such exemptions are implemented within their domestic legal systems (under criminal law or otherwise).

...

"58. For criminal liability to attach, the illegal interception must be committed "intentionally", and "without right". The act is justified, for example, if the intercepting person has the right to do so, if he acts on the instructions or by authorisation of the participants of the transmission (including authorised testing or protection activities agreed to by the participants), or if surveillance is lawfully authorised in the interests of national security or the detection of offences by investigating authorities."

(e) The 2015 Report of the European Commission for Democracy through Law ("the Venice Commission") on the Democratic Oversight of Signals Intelligence Agencies

211. The Venice Commission noted, at the outset, the value that bulk interception could have for security operations, since it enabled the security services to adopt a proactive approach, looking for hitherto unknown dangers rather than investigating known ones. However, it also noted that intercepting bulk data in transmission, or requirements that telecommunications companies store and then provide telecommunications content data or metadata to law-enforcement or security agencies involved an interference with the privacy and other human rights of a large proportion of the population of the world. In this regard, the Venice Commission considered that the main interference with privacy occurred when stored personal data was accessed and/or processed by the agencies. For this reason, the computer analysis (usually with the help of selectors) was one of the important stages for balancing personal integrity concerns against other interests.

212. According to the report, the two most significant safeguards were the authorisation process (of collection and access) and the oversight process. It was clear from the Court's case-law that the latter must be performed by an independent, external body. While the Court had a preference for judicial authorisation, it had not found this to be a necessary requirement. Rather, the system had to be assessed as a whole, and where independent controls were absent at the authorisation stage, particularly strong safeguards had to exist at the oversight stage. In this regard, the Venice Commission considered the example of the system in the United States, where authorisation was given by the Foreign Intelligence Surveillance Court. However, it noted that despite the existence of judicial authorisation, the lack of independent oversight of the court's conditions was problematic.

213. Similarly, the Commission observed that notification of the subject of surveillance was not an absolute requirement of Article 8 of the Convention. In this regard, a general complaints procedure to an independent oversight body could compensate for non-notification.

214. The report also considered internal controls to be a "primary safeguard". In this regard, recruitment and training were key issues; in addition, it was important for the agencies to build in respect for privacy and other human rights when promulgating internal rules.

215. The report also considered the position of journalists. It accepted that they were a group which required special protection, since searching their contacts could reveal their sources (and the risk of discovery could be a powerful disincentive to whistle-blowers). Nevertheless, it considered there to be no absolute prohibition on searching the contacts of journalists, provided that there were very strong reasons for doing so. It acknowledged,

however, that the journalistic profession was not one which was easily identified, since NGOs were also engaged in building public opinion and even bloggers could claim to be entitled to equivalent protections.

216. Finally, the report briefly considered the issue of intelligence sharing, and in particular the risk that States could thereby circumvent stronger domestic surveillance procedures and/or any legal limits which their agencies might be subject to as regards domestic intelligence operations. It considered that a suitable safeguard would be to provide that the bulk material transferred could only be searched if all the material requirements of a national search were fulfilled and this was duly authorised in the same way as a search of bulk material obtained by the signals intelligence agency using its own techniques.

I. European Union law

1. Charter of Fundamental Rights of the European Union

217. Articles 7, 8 and 11 of the Charter provide as follows:

Article 7 – Respect for private and family life

"Everyone has the right to respect for his or her private and family life, home and communications."

Article 8 – Protection of personal data

"1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which have been collected concerning him or her, and the right to have them rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

Article 11 – Freedom of expression and information

"1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

2. The freedom and pluralism of the media shall be respected."

2. EU directives and regulations relating to protection and processing of personal data

218. The Data Protection Directive (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data), adopted on 24 October 1995, regulated for many years the protection and processing of personal data within the European Union. As the activities of Member States regarding public safety,

defence and State security fall outside the scope of Community law, the Directive did not apply to these activities (Article 3(2)).

219. The General Data Protection Regulation, adopted in April 2016, superseded the Data Protection Directive and became enforceable on 25 May 2018. The regulation, which is directly applicable in Member States[1], contains provisions and requirements pertaining to the processing of personally identifiable information of data subjects inside the European Union, and applies to all enterprises, regardless of location, that are doing business with the European Economic Area. Business processes that handle personal data must be built with data protection by design and by default, meaning that personal data must be stored using pseudonymisation or full anonymisation, and use the highest-possible privacy settings by default, so that the data is not available publicly without explicit consent, and cannot be used to identify a subject without additional information stored separately. No personal data may be processed unless it is done under a lawful basis specified by the regulation, or if the data controller or processor has received explicit, opt-in consent from the data's owner. The data owner has the right to revoke this permission at any time.

220. A processor of personal data must clearly disclose any data collection, declare the lawful basis and purpose for data processing, how long data is being retained, and if it is being shared with any third-parties or outside of the EU. Users have the right to request a portable copy of the data collected by a processor in a common format, and the right to have their data erased under certain circumstances. Public authorities, and businesses whose core activities centre around regular or systematic processing of personal data, are required to employ a data protection officer (DPO), who is responsible for managing compliance with the GDPR. Businesses must report any data breaches within 72 hours if they have an adverse effect on user privacy.

221. The Privacy and Electronic Communications Directive (Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector), adopted on 12 July 2002, states, in recitals 2 and 11:

> "(2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.
>
> (11) Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the

[1] As the United Kingdom is leaving the European Union in 2019, it granted royal assent to the Data Protection Act 2018 on 23 May 2018, which contains equivalent regulations and protections.

measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms."

222. The Directive further provides, insofar as relevant:

Article 1 – Scope and aim

"1. This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law."

Article 15 – Application of certain provisions of Directive 95/46/EC

"1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union."

223. On 15 March 2006 the Data Retention Directive (Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and

amending Directive 2002/58/EC) was adopted. It provided, insofar as relevant:

Article 1 - Subject matter and scope

"1. This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

2. This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network."

Article 3 – Obligation to retain data

"1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned."

3. Relevant case-law of the Court of Justice of the European Union ("CJEU")

(a) *Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources and Others and Seitinger and Others* (Cases C-293/12 and C-594/12; ECLI:EU:C:2014:238)

224. In a judgment of 8 April 2014 the Court of Justice of the European Union ("the CJEU") declared invalid the Data Retention Directive 2006/24/EC laying down the obligation on the providers of publicly available electronic communication services or of public communications networks to retain all traffic and location data for periods from six months to two years, in order to ensure that the data was available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. The CJEU noted that, even though the directive did not permit the retention of the content of the communication, the traffic and location data covered by it might allow very precise conclusions to be drawn concerning the private lives of the persons whose data had been retained. Accordingly, the obligation to retain the data constituted in itself an interference with the right to respect for private life and communications guaranteed by Article 7 of the Charter of Fundamental Rights of the EU and the right to protection of personal data under Article 8 of the Charter.

225. The access of the competent national authorities to the data constituted a further interference with those fundamental rights, which the CJEU considered to be "particularly serious". The fact that data was retained and subsequently used without the subscriber or registered user being informed was, according to the CJEU, likely to generate in the minds of the persons concerned the feeling that their private lives were the subject of constant surveillance. The interference satisfied an objective of general interest, namely to contribute to the fight against serious crime and terrorism and thus, ultimately, to public security. However, it failed to satisfy the requirement of proportionality.

226. Firstly, the directive covered, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime. It therefore entailed an interference with the fundamental rights of practically the entire European population. It applied even to persons for whom there was no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime.

227. Secondly, the directive did not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. By simply referring, in a general manner, to serious crime, as defined by each Member State in its national law, the directive failed to lay down any objective criterion by which to determine which offences might be considered to be sufficiently serious to justify such an extensive interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. Above all, the access by the competent national authorities to the data retained was not made dependent on a prior review carried out by a court or by an independent administrative body whose decision sought to limit access to the data and their use to what was strictly necessary for the purpose of attaining the objective pursued.

228. Thirdly, the directive required that all data be retained for a period of at least six months, without any distinction being made between the categories of data on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned. The CJEU concluded that the directive entailed a wide-ranging and particularly serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, without such an interference being precisely circumscribed by provisions to ensure that it was actually limited to what was strictly necessary. The CJEU also noted that the directive did not provide for sufficient safeguards, by means of technical and organisational measures, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of those data.

(b) *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* (Cases C-203/15 and C-698/15; ECLI:EU:C:2016:970)

229. In *Secretary of State for the Home Department v. Watson and Others*, the applicants had sought judicial review of the legality of section 1 of the Data Retention and Investigatory Powers Act 2014 ("DRIPA"), pursuant to which the Secretary of State could require a public telecommunications operator to retain relevant communications data if he considered it necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (h) of section 22(2) of RIPA. The applicants claimed, *inter alia*, that section 1 was incompatible with Articles 7 and 8 of the Charter and Article 8 of the Convention.

230. By judgment of 17 July 2015, the High Court held that the *Digital Rights* judgment laid down "mandatory requirements of EU law" applicable to the legislation of Member States on the retention of communications data and access to such data. Since the CJEU, in that judgment, held that Directive 2006/24 was incompatible with the principle of proportionality, national legislation containing the same provisions as that directive could, equally, not be compatible with that principle. In fact, it followed from the underlying logic of the *Digital Rights* judgment that legislation that established a general body of rules for the retention of communications data was in breach of the rights guaranteed in Articles 7 and 8 of the Charter, unless that legislation was complemented by a body of rules for access to the data, defined by national law, which provides sufficient safeguards to protect those rights. Accordingly, section 1 of DRIPA was not compatible with Articles 7 and 8 of the Charter as it did not lay down clear and precise rules providing for access to and use of retained data and access to that data was not made dependent on prior review by a court or an independent administrative body.

231. On appeal by the Secretary of State, the Court of Appeal sought a preliminary ruling from the CJEU.

232. Before the CJEU this case was joined with the request for a preliminary ruling from the Kammarrätten i Stockholm in Case C‑203/15 *Tele2 Sverige AB v Post- och telestyrelsen*. Following an oral hearing in which some fifteen EU Member States intervened, the CJEU gave judgment on 21 December 2016. The CJEU held that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, had to be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, was not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative

authority, and where there is no requirement that the data concerned should be retained within the European Union.

233. The CJEU declared the Court of Appeal's question whether the protection afforded by Articles 7 and 8 of the Charter was wider than that guaranteed by Article 8 of the Convention inadmissible.

234. Following the handing down of the CJEU's judgment, the case was relisted before the Court of Appeal. On 31 January 2018 it granted declaratory relief in the following terms: that section 1 of DRIPA was inconsistent with EU law to the extent that it permitted access to retained data where the object pursued by access was not restricted solely to fighting serious crime; or where access was not subject to prior review by a court or independent administrative authority.

(c) *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service and Secret Intelligence Service* (IPT/15/110/CH; EU OJ C 22, 22.1.2018, p. 29–30)

235. On 8 September 2017 the IPT gave judgment in the case of *Privacy International*, which concerned the acquisition by the agencies of Bulk Communications Data under section 94 of the Telecommunications Act 1984 (a different regime from those which form the subject of the present complaints) and Bulk Personal Data. The IPT found that, following their avowal, the regimes were compliant with Article 8 of the Convention. However, it identified the following four requirements which appeared to flow from the CJEU judgment in *Watson and Others* and which seemed to go beyond the requirements of Article 8 of the Convention: a restriction on non-targeted access to bulk data; a need for prior authorisation (save in cases of validly established emergency) before data could be accessed; provision for subsequent notification of those affected; and the retention of all data within the European Union.

236. On 30 October 2017 the IPT made a request to the CJEU for a preliminary ruling clarifying the extent to which the *Watson* requirements could apply where the bulk acquisition and automated processing techniques were necessary to protect national security. In doing so, it expressed serious concern that if the *Watson* requirements were to apply to measures taken to safeguard national security, they would frustrate them and put the national security of Member States at risk. In particular, it noted the benefits of bulk acquisition in the context of national security (referring to the Bulk Powers Review – see paragraphs 173-176 above); the risk that the need for prior authorisation could undermine the agencies' ability to tackle the threat to national security; the danger and impracticality of implementing a requirement to give notice in respect of the acquisition or use of a bulk database, especially where national security was at stake; and

the impact an absolute bar on the transfer of data outside the European Union could have on Member States' treaty obligations.

THE LAW

I. EXHAUSTION OF DOMESTIC REMEDIES

237. The Government submitted that the applicants in the first and second of the joined cases had not exhausted domestic remedies within the meaning of Article 35 § 1 of the Convention, which provides as follows:

> "1. The Court may only deal with the matter after all domestic remedies have been exhausted, according to the generally recognised rules of international law, and within a period of six months from the date on which the final decision was taken."

A. The parties' submissions

1. The Government

238. The Government argued that the applicants in the first and second of the joined cases had not exhausted domestic remedies as they had failed to raise their complaints before the IPT. The IPT was a bespoke domestic tribunal set up for the very purpose of investigating, considering and ruling on the issues now raised before this Court. In *Kennedy v. the United Kingdom*, no. 26839/05, 18 May 2010 the Court held that the IPT was Article 6 compliant and, as could be seen from the *Liberty* proceedings, it was capable of providing redress. Furthermore, it was advantageous for the Court to have the benefit of a detailed assessment of the operation of the relevant domestic legal regime by a bespoke domestic tribunal with an understanding of that system. That was especially so where, as in the case at hand, domestic law was not only complex, but also involved an assessment of issues of necessity and proportionality which would be particularly difficult to undertake without a proper determination at national level of facts material to the balance between the rights of the individual and the interests of the community as a whole.

239. As for the effectiveness of the IPT as a domestic remedy, the Government noted that it was "one of the most far-reaching systems of judicial oversight over intelligence matters in the world", with broad jurisdiction and remedial powers. It produced open judgments to the extent that it could do so consistently with the public interest. It could investigate and consider in closed session any sensitive material that was relevant to the complaints and produce decisions having regard to that material. On account of its ability to assess and evaluate the adequacy of the internal safeguards, it was in a "special position" to make a proper assessment of

proportionality. In the present case, the applicants' complaints under Articles 8 and 10 of the Convention focussed on the alleged lack of publicly available safeguards and proportionality, and the IPT had the jurisdiction and requisite powers to deal with all of those complaints. It could make clear the extent to which the relevant domestic regime was compatible with the Convention and, if it was not compatible, it could identify the respects in which it was deficient. If there was a lack of foreseeability, it could identify with precision the respects in which the applicable safeguards were not – but should be – public, which, in turn, meant that those aspects of the regime could be remedied by the Government with further disclosure and/or amendments to the Code of Practice. Finally, where proportionality was in issue, it could, through its ability to consider relevant intelligence material in closed proceedings, provide an effective remedy by ordering the quashing of section 8(4) warrants and ordering the destruction of data.

240. Finally, in relation to the IPT's more general declaratory jurisdiction, the Government argued that there was no deficit in Convention terms. On the contrary, it could and did rule on the general lawfulness of regimes about which complaints were made and if it concluded that a regime was contrary to the Convention, it would so state. Furthermore, the Government's reaction to such findings had been consistent. As could be seen from the response to the *Liberty* and *Belhadj* determinations (see paragraphs 92-94 above), it had ensured that any defects were rectified and dealt with. Therefore, even though it has no jurisdiction to make a Declaration of Incompatibility under section 4 of the Human Rights Act 1998, on the facts a finding of incompatibility would be an effective trigger for the necessary changes to ensure Convention compatibility. In light of both this fact, and the Court's increasing emphasis on subsidiarity, the Government contended that the position had moved on since *Kennedy*, in which the Court did not accept that the IPT had provided the applicant with an effective remedy for his general complaint about the Convention compliance of section 8(1) of RIPA.

2. The applicants

241. The applicants in the first and second of the joined cases submitted that they had done all that was required of them in terms of domestic remedies. While they accepted that they did not file complaints with the IPT before lodging their applications with this Court, they had not done so in reliance on the Court's findings in *Kennedy*; namely, that a claim before the IPT was not necessary in order for a general challenge to be brought against the United Kingdom's domestic framework. Although they accepted that it was always open to the Court to reconsider whether a domestic avenue of complaint provided an effective remedy, it had held that an applicant could only be required to make use of a remedy that had developed since the application was lodged if they could still make use of the remedy and it

would not be unjust to declare the application admissible (*Campbell and Fell v. the United Kingdom*, 28 June 1984, §§ 62-63, Series A no. 80).

242. In any event, the applicants argued that there had been no change of circumstances such as would make the IPT an effective remedy. In particular, they relied upon the arguments made by the applicants in the third of the joined cases in support of their Article 6 complaint, and further noted that the IPT could not make a Declaration of Incompatibility. The latter in any case did not constitute an effective remedy, since it did not result in the invalidation of the impugned legislation).

B. The submissions of the third party

243. In its third party intervention, the European Network of National Human Rights Institutions ("ENNHRI") submitted that the international legal framework, including the International Covenant on Civil and Political Rights ("ICCPR") and the American Convention on Human Rights ("ACHR"), and case-law supported the contention that domestic remedies did not have to be followed if they were not capable of providing an effective remedy.

C. The Court's assessment

1. General principles

244. It is a fundamental feature of the machinery of protection established by the Convention that it is subsidiary to the national systems safeguarding human rights. This Court is concerned with the supervision of the implementation by Contracting States of their obligations under the Convention. It should not take on the role of Contracting States, whose responsibility it is to ensure that the fundamental rights and freedoms enshrined therein are respected and protected on a domestic level (*Vučković and Others v. Serbia* (preliminary objection) [GC], nos. 17153/11 and 29 others, § 69, 25 March 2014). However, the application of the rule must make due allowance for the fact that it is being applied in the context of machinery for the protection of human rights that the Contracting Parties have agreed to set up and it must therefore be applied with some degree of flexibility and without excessive formalism (see *Vučković and Others*, cited above, § 76; see also *Akdivar and Others v. Turkey*, 16 September 1996, § 69, *Reports of Judgments and Decisions* 1996-IV and *Gough v. the United Kingdom*, no. 49327/11, § 140, 28 October 2014).

245. States are dispensed from answering before an international body for their acts before they have had an opportunity to put matters right through their own legal system, and those who wish to invoke the supervisory jurisdiction of the Court as concerns complaints against a State

are thus obliged to use first the remedies provided by the national legal system (see, among many authorities, *Vučković and Others*, cited above, § 70 and *Akdivar and Others*, cited above, § 65). The Court is not a court of first instance; it does not have the capacity, nor is it appropriate to its function as an international court, to adjudicate on cases which require the finding of basic facts, which should, as a matter of principle and effective practice, be the domain of domestic jurisdiction (see *Demopoulos and Others v. Turkey* (dec.) [GC], nos. 46113/99, 3843/02, 13751/02, 13466/03, 10200/04, 14163/04, 19993/04 and 21819/04, § 69, ECHR 2010). Similarly, in cases requiring the balancing of conflicting interests under Articles 8 and 10 of the Convention it is particularly important that the domestic courts are first given the opportunity to strike the "complex and delicate" balance between the competing interests at stake. Those courts are in principle better placed than this Court to make such an assessment and, as a consequence, their conclusions will be central to its own consideration of the issue (*MGN Limited v. the United Kingdom*, no. 39401/04, §§ 140-155, 18 January 2011; *Palomo Sánchez and Others v. Spain* [GC], nos. 28955/06, 28957/06, 28959/06 and 28964/06, § 57, 12 September 2011; *Axel Springer AG v. Germany* [GC], no. 39954/08, §§ 85-88, 7 February 2012; *Courtney v. Ireland* (dec), no. 69558/10, 18 December 2012; and *Charron and Merle-Montet v. France* (dec), no. 22612/15, § 30, 16 January 2018).

246. The obligation to exhaust domestic remedies therefore requires an applicant to make normal use of remedies which are available and sufficient in respect of his or her Convention grievances. The existence of the remedies in question must be sufficiently certain not only in theory but in practice, failing which they will lack the requisite accessibility and effectiveness (see *Vučković and Others*, cited above, § 71 and *Akdivar and Others*, cited above, § 66).

247. There is, however, no obligation to have recourse to remedies which are inadequate or ineffective. To be effective, a remedy must be capable of remedying directly the impugned state of affairs and must offer reasonable prospects of success (see *Vučković and Others*, cited above, § 73 and *Sejdovic v. Italy* [GC], no. 56581/00, § 46, ECHR 2006‑II). The existence of mere doubts as to the prospects of success of a particular remedy which is not obviously futile is not a valid reason for failing to exhaust that avenue of redress (see *Vučković and Others*, cited above, § 74 and *Scoppola v. Italy (no. 2)* [GC], no. 10249/03, § 70, 17 September 2009).

248. As regards the burden of proof, it is incumbent on the Government claiming non-exhaustion to satisfy the Court that the remedy was an effective one, available in theory and in practice at the relevant time. Once this burden has been satisfied, it falls to the applicant to establish that the remedy advanced by the Government was in fact exhausted, or was for some reason inadequate and ineffective in the particular circumstances of

the case, or that there existed special circumstances absolving him or her from this requirement (see *Vučković and Others*, cited above, § 77; *McFarlane v. Ireland* [GC], no. 31333/06, § 107, 10 September 2010; *Demopoulos and Others*, cited above, § 69; and *Akdivar and Others*, cited above, § 68).

249. Where an applicant is challenging the general legal framework for secret surveillance measures, the Court has identified the availability of an effective domestic remedy as a relevant factor in determining whether that applicant was a "victim" of the alleged violation, since, in the absence of such a remedy, widespread suspicion and concern among the general public that secret surveillance powers were being abused might be justified (*Roman Zakharov v. Russia* [GC], no. 47143/06, § 171, ECHR 2015).

2. Application of those principles to the case at hand

250. The IPT is a specialist tribunal with sole jurisdiction to hear allegations of wrongful interference with communications as a result of conduct covered by RIPA (see paragraph 124 above). The Court of Appeal has recently observed that the IPT is "a judicial body of like standing and authority to the High Court" and that "[t]he quality of the membership of the IPT in terms of judicial expertise and independence is very high" (see paragraph 135 above). Its members must hold or have held high judicial office or be a qualified lawyer of at least ten years' standing (see paragraph 123 above), and in the present case it was composed of two High Court Judges (including the President), a Circuit Judge and two senior barristers (see paragraph 24 above). It has jurisdiction to investigate any complaint that a person's communications have been intercepted (see paragraph 124 above). In conducting such an investigation, the IPT will generally proceed on the assumption that the facts asserted by the applicant are true and then, acting upon that assumption, decide whether they would constitute lawful or unlawful conduct. In doing so, the IPT considers both the generic compliance of the relevant interception regime (on the basis of assuming there to have been an interception as alleged) as well as, at a subsequent stage, the specific question whether the individual applicant's rights have, in fact, been breached. Those involved in the authorisation and execution of an intercept warrant are required to disclose to the IPT all the documents it may require, including "below the waterline" documents which could not be made public for reasons of national security (see paragraph 127 above), irrespective of whether those documents support or undermine their defence. The IPT has discretion to hold oral hearings, in public, where possible (see paragraphs 131, 138 and 139 above) and, in closed proceedings it may appoint Counsel to the Tribunal to make submissions on behalf of claimants who cannot be represented (see paragraph 142 above). When it determines a complaint the IPT has the power to award compensation and make any other order it sees fit, including

quashing or cancelling any warrant and requiring the destruction of any records (see paragraph 128 above). In considering the complaint brought by the applicants in the third of the joined cases ("the *Liberty* proceedings"), the IPT used all of these powers for the benefit of the applicants.

251. The Court considered the role of the IPT in secret surveillance cases in *Kennedy* (cited above), decided in 2010. In that case the applicant complained that his communications had been intercepted pursuant to a targeted warrant authorised under section 8(1) of RIPA (the specific complaint), and that the targeted interception regime under section 8(1) was not compliant with Article 8 of the Convention (the general compliance complaint). The Court held that the proceedings before the IPT had been Article 6 compliant, since any procedural restrictions were proportionate to the need to keep secret sensitive and confidential information and did not impair the very essence of the applicant's right to a fair trial. With regard to the IPT's effectiveness as a remedy, it acknowledged that Article 35 § 1 had "a special significance in the context of secret surveillance given the extensive powers of the IPT to investigate complaints before it and to access confidential information". It considered these extensive powers to be relevant to the applicant's specific complaint as it had required a factual investigation into whether his communications had been intercepted. However, it was not persuaded of their relevance to the general compliance complaint, since it was a legal challenge and, having already decided the specific complaint, it was unlikely that the IPT could further elucidate the general operation of the surveillance regime and applicable safeguards, such as would assist the Court in its consideration of the compliance of the regime with the Convention. While it accepted that the IPT could consider a complaint about the general compliance of a surveillance regime with the Convention and, if necessary, make a finding of incompatibility, the Government had not addressed in their submissions how such a finding would benefit the applicant, given that it did not appear to give rise to a binding obligation on the State to remedy the incompatibility.

252. Although in *Kennedy* the Court distinguished between a specific and general complaint, it is clear from its more recent case-law that while the two complaints are indeed distinct, they are nevertheless connected. In *Roman Zakharov* the Court identified the availability of an effective domestic remedy to a person who suspects that he or she was subjected to secret surveillance (in other words, an effective domestic remedy for a specific complaint) as a relevant factor in determining whether that person was a "victim" in respect of a complaint challenging the general legal framework for secret surveillance, since, in the absence of such a remedy, widespread suspicion and concern among the general public that secret surveillance powers were being abused might be justified (*Roman Zakharov*, cited above, § 171). In view of the significance the Court has attached to the existence of such a domestic remedy, it would be

problematic if applicants were not required to use it before making either a specific or general complaint to this Court. The Court should not have to consider a challenge to a legislative regime *in abstracto* when the applicants had a domestic forum in which they could have challenged at the very least the possible application of those measures to them.

253. In any event, the IPT's ruling in Mr Kennedy's case came very early in the Tribunal's history. In fact, Mr Kennedy's application, together with an application lodged by British and Irish Rights Watch, was the first time that the IPT sat in public. It was in the context of those applications that it gave its defining ruling on preliminary issues of law and established its current practice (see paragraphs 136-141 above). For the reasons set out below, the Court considers that in view both of the manner in which the IPT has exercised its powers in the fifteen years that have elapsed since that ruling, and the very real impact its judgments have had on domestic law and practice, the concerns expressed by the Court in *Kennedy* about its effectiveness as a remedy for complaints about the general compliance of a secret surveillance regime are no longer valid.

254. First, in *Kennedy* the IPT had fully examined Mr Kennedy's specific complaint about the interception of his communications. The Court was solely concerned with whether an examination of the general complaint could have provided additional clarification. Unlike the present case, therefore, the Court was not being called upon to consider the general complaint entirely *in abstracto*.

255. Secondly, an examination of the IPT's extensive post-*Kennedy* case-law demonstrates the important role that it can and does play in analysing and elucidating the general operation of secret surveillance regimes. For example, in *B v. the Security Services*, Case No IPT/03/01/CH, 21 March 2004 the IPT considered, as a preliminary issue of law, whether the Secretary of State's "neither confirm nor deny" policy was compatible with Article 8 of the Convention. Similarly, in *A Complaint of Surveillance*, Case No IPT/A1/2013, 24 July 2013 the IPT provided elucidation on the meaning of the term "surveillance" in Part II of RIPA. Moreover, given the "secret" nature of most surveillance regimes, the scope of their operation will not always be evident from the "above the waterline" material. For example, in the *Liberty* proceedings the IPT played a crucial role first in identifying those aspects of the surveillance regimes which could and should be further elucidated, and then recommending the disclosure of certain "below the waterline" arrangements in order to achieve this goal. It could therefore be said that the IPT, as the only tribunal with jurisdiction to obtain and review "below the waterline" material, is not only the sole body capable of elucidating the general operation of a surveillance regime; it is also the sole body capable of determining whether that regime requires further elucidation.

256. This "elucidatory" role is of invaluable assistance to the Court when it is considering the compliance of a secret surveillance regime with the Convention. The Court has repeatedly stated that it is not its role to determine questions of fact or to interpret domestic law. That is especially so where domestic law is complex and, for reasons of national security, the State is not at liberty to disclose relevant information to it. Given the confidential nature of the relevant documentation, were applicants to lodge complaints about secret surveillance with this Court without first raising them before the IPT, this Court would either have to become the primary fact-finder in such cases, or it would have to assess necessity and proportionality in a factual vacuum. This difficulty is particularly apparent in respect of those complaints not considered by the IPT in the *Liberty* proceedings; in particular, the Chapter II complaint and the complaint about the receipt of non-intercept material from foreign intelligence services. The Court has before it very limited information about the scope and operation of these regimes and it could therefore only consider these complaints if it were either to accept the applicants' allegations as fact, or to attempt to conduct its own fact-finding exercise. In such cases, therefore, it is particularly important that the domestic courts, which have access to the confidential documentation, first strike the "complex and delicate balance" between the competing interests at stake (see paragraph 245 above).

257. Consequently, on the basis of the information submitted to it, the Court considers that the IPT can – and regularly does – elucidate the general operation of surveillance regimes, including in cases where such elucidation is considered necessary to ensure the regime's Convention compliance.

258. Furthermore, from the information submitted in the present case it would appear that where the IPT has found a surveillance regime to be incompatible with the Convention, the Government have ensured that any defects are rectified and dealt with. In the *Liberty* proceedings, once the IPT had identified which of the "below the waterline" arrangements could and should be made public in order for the intelligence sharing regime to be Convention compliant, the Government agreed to the proposed disclosure ("the 9 October disclosure") and the disclosed material was subsequently added to the amended Code of Practice (see paragraphs 26-30 above). In addition, having found that there had been a breach of Article 8 of the Convention by virtue of the fact that email communications of Amnesty International, which had been intercepted and accessed "lawfully and proportionately", had nevertheless been retained for longer than was permitted under GCHQ's internal policies, the IPT ordered GCHQ to destroy the communications within seven days, and to provide a closed report within fourteen days confirming their destruction (see paragraph 54 above).

259. Similarly, in the *Belhadj* case the Government conceded that from January 2010 the regime for the interception, obtaining, analysis, use,

disclosure and destruction of legally privileged material had not been in accordance with the law for the purposes of Article 8 § 2 of the Convention and was accordingly unlawful. As a consequence, the Security Service and GCHQ confirmed that they would work in the forthcoming weeks to review their policies and procedures (see paragraph 93 above).

260. In addition, in *News Group and Others v. The Commissioner of Police of the Metropolis* the IPT found that the regime under Chapter II of RIPA (for the acquisition of communications data) did not contain effective safeguards to protect Article 10 rights. Although the IPT could not award any remedy in respect of the failure to provide adequate safeguards, as this did not in itself render the authorisations for the acquisition of communications data unlawful, in March 2015 the 2007 ACD Code of Practice was replaced by a new code with enhanced safeguards in respect of applications for communications data designed to identify a journalist's source (see paragraphs 118-120 above). The applicants in that case subsequently lodged a complaint under Article 10 of the Convention with this Court; however, in a recent decision the Court declared the complaint inadmissible as it found that the applicants had not suffered a "significant disadvantage" within the meaning of Article 35 § 3 (b) of the Convention (see *Anthony France and Others v. the United Kingdom* (dec.), nos. 25357/16, 25514/16, 25552/16 and 25597/16, 26 September 2016). In particular, the Court observed that "the applicants have benefitted from a thorough and comprehensive judgment from the IPT, which clearly sets out all the aspects of the interference with their rights". Furthermore, although "the IPT could not find that there had been a violation of their rights, it nonetheless made a clear statement that their rights had been infringed" and a change in the law subsequently occurred (see *Anthony France and Others*, cited above, §§ 43-46).

261. Finally, to cite an earlier example, in *Paton and Others v. Poole Borough Council*, Case Nos IPT/09/01/C, IPT/09/02/C, IPT/09/03/C, IPT/09/04/C and IPT/09/05/C, 29 July 2010, the IPT found that surveillance carried out by a local authority was both unlawful and in breach of Article 8 of the Convention as it was not for the permitted purpose and was neither necessary nor proportionate. While the IPT made no findings regarding the Convention compliance of the regime as a whole, the case was highly publicised and fed into a general public debate about the surveillance powers of local councils. Very shortly after the judgment was handed down, the Government announced that there was to be a review of RIPA which would cover its use by local authorities. Two years later RIPA was amended to restrict the power of local authorities to conduct surveillance.

262. Therefore, while the evidence submitted by the Government may not yet demonstrate the existence of a "binding obligation" requiring it to remedy any incompatibility identified by the IPT, in light of the IPT's "special significance" in secret surveillance cases which arises from its

"extensive powers ... to investigate complaints before it and to access confidential information" (see *Kennedy*, cited above, § 110) the Court would nevertheless accept that the practice of giving effect to its findings on the incompatibility of domestic law with the Convention is sufficiently certain for it to be satisfied as to the effectiveness of the remedy.

263. The effectiveness of the IPT is further underlined by the fact that it can, as a matter of EU law, make an order for reference to the CJEU where an issue arises that is relevant to the dispute before it (see *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service and Secret Intelligence Service*, at paragraph 236 above). The Court has held that the protection of fundamental rights by Community law can be considered to be "equivalent" to that of the Convention system (see *Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi v. Ireland* [GC], no. 45036/98, § 165 ECHR 2005-VI) and it would therefore be surprising if applicants were permitted to bypass a court or tribunal which could have such a significant role in the enforcement of Community law and its fundamental rights guarantees.

264. Insofar as the applicants rely on the fact that the IPT cannot issue a Declaration of Incompatibility (see paragraph 242 above), it is sufficient to note that the Court has not yet accepted that the practice of giving effect to the national courts' Declarations of Incompatibility by amendment of legislation is "so certain as to indicate that section 4 of the Human Rights Act is to be interpreted as imposing a binding obligation" (see *Burden v. the United Kingdom* [GC], no. 13378/05, § 43, ECHR 2008). Consequently, the relevant question is not whether the IPT can issue a Declaration of Incompatibility, but whether the practice of giving effect to its findings is sufficiently certain.

265. In light of the foregoing considerations, the Court finds that as a general rule the IPT has shown itself to be a remedy, available in theory and practice, which is capable of offering redress to applicants complaining of both specific incidences of surveillance and the general Convention compliance of surveillance regimes. As a result, the complaints made by the applicants in the first and second of the joined cases must be declared inadmissible for non-exhaustion unless they can show that there existed special circumstances absolving them from the requirement to exhaust this remedy.

266. In this regard, they contend that precisely such circumstances existed; namely, that at the time they lodged their applications with this Court they were entitled to rely on *Kennedy* as authority for the proposition that the IPT was not an effective remedy for a complaint about the general Convention compliance of a surveillance regime.

267. Although, at first glance, there would appear to be significant differences between the present case and that of *Kennedy* (for example, as the applicant in *Kennedy* had brought a specific complaint to the IPT the Court was not required to consider the more general complaint entirely in the abstract, and in *Kennedy* the applicant's challenge to the RIPA provisions was a challenge to primary legislation as opposed to the whole legal framework governing the relevant surveillance regime), the Government, for their part, have not sought to distinguish *Kennedy* from the case at hand. Moreover, the case-law of the IPT which the Government have relied on as evidence of its effectiveness as a remedy post-dates the introduction before this Court – on 4 September 2013 and 11 September 2014 – of the complaints made by the applicants in the first and second of the joined cases. For example, the main judgment in the *Liberty* proceedings was delivered on 5 December 2014, the *Belhadj* proceedings concluded on 26 February 2015 and *News Group and Others* was decided on 17 December 2015). While the Court has identified some earlier cases which illustrate the effectiveness of the IPT (for example, *B*, *A Complaint of Surveillance* and *Paton and Others*), none of these cases concerned a general complaint about the Convention compliance of a surveillance regime. In comparison, the *Liberty* proceedings, *Belhadj* and *News Group and Others* all demonstrate the important and unique role of the IPT in both elucidating the operation of such regimes, and remedying any breaches of the Convention.

268. Consequently, while the Court acknowledges that since *Kennedy* was decided in 2010 the IPT has shown itself to be an effective remedy which applicants complaining about the actions of the intelligence services and/or the general operation of surveillance regimes should first exhaust in order to satisfy the requirements of Article 35 § 1 of the Convention, it would nevertheless accept that at the time the applicants in the first and second of the joined cases introduced their applications, they could not be faulted for relying on *Kennedy* as authority for the proposition that the IPT was not an effective remedy for a complaint about the general Convention compliance of a surveillance regime. It therefore finds that there existed special circumstances absolving these applicants from the requirement that they first bring their complaints to the IPT and, as a consequence, it considers that their complaints cannot be declared inadmissible pursuant to Article 35 § 1 of the Convention.

II. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

269. Cumulatively, the applicants in the three joined cases complain about the Article 8 compatibility of three discrete regimes: the regime for the bulk interception of communications under section 8(4) of RIPA; the intelligence sharing regime; and the regime for the acquisition of

communications data under Chapter II of RIPA. The Court will consider each of these regimes separately.

A. The section 8(4) regime

270. The applicants in all of the joined cases complain that the regime under section 8(4) of RIPA for the bulk interception of communications is incompatible with their right to respect for their rights under Article 8 of the Convention, which reads as follows:

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

271. The Government contested that argument. They did not, however, raise any objection under Article 1 of the Convention; nor did they suggest that the interception of communications under the section 8(4) regime was taking place outside the United Kingdom's territorial jurisdiction. The Court will therefore proceed on the assumption that the matters complained of fall within the jurisdictional competence of the United Kingdom.

1. Admissibility

272. The Court notes that this complaint is not manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention. It further notes that it is not inadmissible on any other grounds. It must therefore be declared admissible.

2. Merits

(a) The parties' submissions

(i) The applicants

273. The applicants accepted that the bulk interception regime had a basis in domestic law. However, they argued that it lacked the quality of law because it was so complex as to be inaccessible to the public and to the Government, reliance was placed on arrangements which were substantially "below the waterline" rather than on clear and binding legal guidelines, and it lacked sufficient guarantees against abuse.

274. In particular, the applicants submitted that the section 8(4) regime did not comply with the six requirements identified by this Court in *Weber and Saravia v. Germany* (dec.), no. 54934/00, ECHR 2006‑XI. Firstly, they contended that the purposes for which interception could be permitted (such

as "the interests of national security" and "the economic well-being of the United Kingdom) were too vague to provide a clear limit on the intelligence services' activities.

275. Secondly, they argued that in practice any person was liable to have his or her communications intercepted under section 8(4). Although the regime was targeted at "external" communications, there was no clear definition of "internal" and "external" communications, and in any event modern technological developments had rendered the distinction between the two meaningless. While the Secretary of State was required to provide descriptions of the material he considered it necessary to examine, the ISC had reported that section 8(4) warrants were framed in generic terms.

276. Thirdly, with regard to the limits on the duration of surveillance, the applicants submitted that, in practice, a section 8(4) warrant could continue indefinitely, being renewed every six months by the Secretary of State pursuant to section 9(1)(b) of RIPA.

277. Fourthly, according to the applicants the procedure for filtering, storing and analysing intercepted material lacked adequate safeguards and gave rise to an unacceptable risk of an arbitrary and disproportionate interference with Article 8 of the Convention. First of all, there was no requirement that the selectors used to filter intercepted communications be identified in the Secretary of State's certificate accompanying the section 8(4) warrant, and these selectors were not otherwise subject to oversight. Secondly, the section 16 safeguards only applied where a person was "known to be for the time being in the British Islands". Thirdly, the protections in section 16 of RIPA only applied to the "content" of intercepted communications, and not the filtering, storage and analysis of "related communications data", despite the fact that communications data was capable of providing the Government with a detailed profile of the most intimate aspects of a person's private life.

278. Fifthly, in relation to the communication of intercepted material, the applicants contended that the requirement that the Secretary of State ensure that its disclosure was limited to "the minimum that is necessary for the authorised purposes" was an ineffective safeguard. The authorised purposes enumerated in section 15(4) of RIPA were extremely wide, and included situations where the information was or was "likely to become" necessary for any of the purposes specified in section 5(3) of RIPA.

279. Sixth and finally, the applicants submitted that there were no effective or binding safeguards against the disproportionate retention of intercepted data. Indeed, according to the applicants it was clear from the third IPT judgment in the *Liberty* proceedings that Amnesty International's communications had been stored without the appropriate (automated) deletion procedures being followed, and neither the intelligence services nor the oversight and audit mechanisms had detected this.

280. In addition to arguing that the *Weber* requirements were not satisfied, the applicants in any event contended that they were no longer sufficient to ensure that a communications surveillance regime was compatible with Article 8 of the Convention. *Weber* had been decided in 2006, and subsequent technological developments meant that Governments could now create detailed and intrusive profiles of intimate aspects of private lives by analysing patterns of communications on a bulk basis. The applicants therefore identified a number of additional requirements which they believed were now necessary to ensure the Convention compliance of a legal framework for surveillance: the requirement for objective evidence of reasonable suspicion in relation to the persons for whom data was being sought; prior independent judicial authorisation of interception warrants; and the subsequent notification of the surveillance subject.

281. Finally, the applicants submitted that the section 8(4) regime was disproportionate. In their view the intelligence services were systematically collecting both content and communications data on a massive scale and retaining it for future searching and use. Such a blanket approach fell foul of the principles established in *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, ECHR 2008 and *M.K. v. France*, no. 19522/09, 18 April 2013.

(ii) The Government

282. At the outset, the Government submitted that the information and intelligence obtained under the section 8(4) regime was critical to the protection of the United Kingdom from national security threats; in particular, but not exclusively, from the threat of terrorism. This was especially so given the current level of sophistication of terrorists and criminals in communicating over the Internet in ways that avoided detection, whether through the use of encryption, the adoption of bespoke communications systems, or simply because of the volume of Internet traffic in which they could now hide their communications. Imposing additional fetters on the interception of communications would damage the State's ability to safeguard national security and combat serious crime at exactly the point when advances in communication technology had increased the threat from terrorists and criminals using the Internet.

283. The seriousness of the terrorist threat was underscored by a number of recent attacks across the United Kingdom and Europe, including the attack on Westminster Bridge on 22 March 2017, the Manchester Arena bombing of 22 May 2017, the attack on London Bridge on 3 June 2017, the attacks in Barcelona and Cambrils on 17 August 2017, and the attack on the London Underground on 15 September 2017. The Government therefore submitted that under the Convention scheme, it was properly for States to judge what was necessary to protect the general community from such threats. While those systems were subject to the Court's scrutiny, it had

consistently – and rightly – afforded States a broad margin of appreciation in this field so as not to undermine the effectiveness of systems for obtaining life-saving intelligence that could not be gathered any other way.

284. Although the Government denied that the section 8(4) regime permitted mass surveillance or generalised access to communications, it accepted that it permitted, pursuant to the lawful authority of warrants, the bulk interception of bearers for wanted external communications. In the Government's opinion, the distinction between "internal" and "external" communications was sufficiently clear, and in any event it operated primarily as a safeguard at the macro level; that is, in determining which bearers should be targeted for interception. The Government further contended that bulk interception was critical for the discovery of threats and hitherto unknown targets which might be responsible for threats. Even when the identity of targets was known, they were likely to use a variety of different means of communication, and change those means frequently. Electronic communications did not traverse the Internet by routes that could necessarily be predicted; rather, they took the most efficient route, determined by factors such as cost and the volume of traffic passing over particular parts of the Internet at different times of the day. In addition, communications sent over the Internet were broken down into small pieces (or "packets"), which were transmitted separately, often through different routes. In the opinion of the Government, it was therefore necessary to intercept all communications travelling over more than one bearer to maximise the chance of identifying and obtaining the communications being sent to known targets.

285. With regard to whether the interference complained of was "in accordance with the law", the Government relied on the fact that it had its basis in primary legislation, namely section 8(4) of RIPA, supplemented by the Interception of Communications Code of Practice ("the IC Code"). It had been further clarified by the reports of the Interception of Communications Commissioner, which were also public documents.

286. In relation to the *Weber* requirements the Government argued that the first foreseeability requirement, being the "offences" which might give rise to an interception order, was satisfied by section 5 of RIPA, which defined the purposes for which the Secretary of State could issue an interception warrant. In *Kennedy*, despite the applicant's criticism of the terms "national security" and "serious crime", the Court had found the description of the offences which might give rise to an interception order to be sufficiently clear (*Kennedy*, cited above, § 159).

287. Relying on *Weber*, the Government submitted that the second foreseeability requirement (the categories of people liable to have their communications intercepted) applied at both the interception stage and the selection stage. As regards the interception stage, a section 8(4) warrant was targeted at "external" communications, although in principle it might

authorise the interception of "internal" communications insofar as that was necessary in order to intercept the external communications to which the warrant related. With regard to the selection stage, section 16(1) of RIPA provided that no intercepted material could be read, looked at or listened to by any person unless it fell within the Secretary of State's certificate, and it was proportionate in the circumstances to do so. Furthermore, section 16(2) placed sufficiently precise limits on the extent to which intercepted material could be selected to be read, looked at or listened to according to a factor which was referable to an individual known to be for the time being in the British Islands and which had as (one of) its purpose(s) the identification of material contained in communications sent by or intended for him.

288. The Government further argued that paragraphs 6.22-6.24 of the IC Code made sufficient provision for the duration and renewal of a section 8(4) warrant, thereby complying with the third requirement identified in *Weber*. Pursuant to section 9(2) of RIPA, a section 8(4) warrant could only be renewed if the Secretary of State believed that it continued to be necessary, and if the Secretary of State believed that the warrant was no longer necessary, section 9(3) of RIPA required that it be cancelled.

289. According to the Government, insofar as intercepted material could not be read, looked at or listened to by a person pursuant to section 16 of RIPA, it could not be used at all. Prior to its destruction, paragraph 7.7 of the IC Code required that it be stored securely. For material that could be read, looked at and listened to pursuant to section 16, the Government submitted that the regime satisfied the fourth of the *Weber* requirements. In particular, material had to be selected for examination through the application of search terms by equipment operating automatically for that purpose. If an analyst then wished to select material for examination, paragraphs 7.14-7.16 of the IC Code required that he or she create a record setting out why access was required and proportionate, consistent with the applicable certificate, and stating any circumstances likely to give rise to a degree of collateral infringement of privacy, and any measures taken to reduce the extent of that infringement. That record had to be retained for the purpose of subsequent audit. Paragraphs 7.11-7.20 further required that material should only be read, looked at or listened to by authorised persons receiving regular training in the operation of section 16 of RIPA and the requirements of necessity and proportionality. Finally, material could only be used by the intelligence services in accordance with their statutory functions, and only insofar as was proportionate under section 6(1) of the Human Rights Act 1998.

290. The Government further submitted that the section 8(4) regime satisfied the fifth *Weber* requirement. Section 15(2) set out the precautions to be taken when communicating intercepted material to other people. These precautions served to ensure that only so much intercepted material as was "necessary" for the authorised purpose could be disclosed. Paragraphs 7.4

and 7.5 of the IC Code further provided that where intercepted material was to be disclosed to a foreign State, the intelligence services had to take reasonable steps to ensure that the authorities of that State had and would maintain the necessary procedures to safeguard the intercepted material, and to ensure that it was disclosed, copied, distributed and retained only to the minimum extent necessary. It could only be further disclosed to the authorities of a third country if explicitly agreed. Finally, any disclosure would have to satisfy the constraints imposed by sections 1-2 of the Security Services Act 1989, sections 1-4 of the Intelligence Services Act 1994 as read with section 19(3)-(5) of the Counter Terrorism Act 2008 and section 6(1) of the Human Rights Act 1998.

291. With regard to the final *Weber* requirement, the Government contended that section 15(3) of RIPA and paragraphs 7.8-7.9 of the IC Code made sufficient provision for the circumstances in which intercepted material had to be erased or destroyed (including the obligation to review retention at appropriate intervals, and the specification of maximum retention periods which should normally be no longer than two years).

292. Although the Government acknowledged that the safeguards in section 16 of RIPA did not apply to "related communications data", they argued that the covert acquisition of related communications data was less intrusive than the covert acquisition of content and, as such, the Court had never applied the *Weber* requirements to powers to acquire communications data. It was therefore their contention that instead of the list of six specific foreseeability requirements, the test in respect of communications data should be the more general one of whether the law indicated the scope of any discretion and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.

293. According to the Government, the section 8(4) regime satisfied this test as regards the obtaining and use of related communications data. First of all, "related communications data" as defined in sections 20 and 21 of RIPA was not synonymous with "metadata" but was instead a limited subset of metadata. Secondly, the section 8(4) regime was sufficiently clear as to the circumstances in which the intelligence services could obtain related communications data (namely, by the interception of bearers pursuant to a section 8(4) warrant). Once obtained, access to related communications data had to be necessary and proportionate under section 6(1) of the Human Rights Act 1998 and subject to the constraints in sections 1-2 of the Security Services Act and sections 1-4 of the Intelligence Services Act. Storage, handling, use and disclosure of related communications data, including access by a foreign intelligence partner, would be constrained by section 15 of RIPA and paragraphs 7.1-7.10 of the IC Code. Finally, the Government argued that there was good reason for exempting related communications data from the safeguards in section 16; in order for section 16 to work, the

intelligence services needed to be able to assess whether a potential target was "for the time being in the British Islands".

294. Finally, the Government addressed the applicants' proposals for "updating" the *Weber* requirements. They submitted that any requirement of "reasonable suspicion" would largely preclude the operation of bulk interception regimes, despite the fact that the Court had permitted such monitoring in *Weber*. Furthermore, in *Kennedy* (cited above, § 167) the Court clearly held that judicial authorisation could be either *ex ante* or *post facto*. In that case the Court had found that the oversight provided by the Commissioner, the ISC and the IPT had compensated for any lack of prior judicial authorisation. Finally, any requirement to notify a suspect of the use of bulk data tools against him could fundamentally undermine the work of the intelligence services and potentially threaten the lives of covert human intelligence sources close to the suspect. It would also be wholly impractical in the section 8(4) context, since many of the targets would be overseas and their personal details might be unknown or imperfectly known.

(b) The submissions of the third parties

(i) Article 19

295. Article 19 submitted that mass interception powers were by their very nature inherently incapable of being exercised in a proportionate manner and, as such, were inherently incompatible with the requirements of the Convention. Article 19 therefore urged the Court to conclude that only targeted surveillance based on reasonable suspicion and authorised by a judge constituted a legitimate restriction on the right to privacy.

(ii) Access Now

296. Access Now submitted that the mass surveillance at issue in the present case failed to comply with the International Covenant on Civil and Political Rights ("ICCPR") and the International Principles on the Application of Human Rights to Communications Surveillance since the United Kingdom had not demonstrated that such surveillance was strictly necessary or proportionate. They further contended that surveillance programmes should not be considered independently but should instead be viewed in relation to the entirety of a nation's surveillance activities as machine learning, through which mathematical algorithms could draw inferences from collections of data, had increased the invasiveness of big data sets and data mining.

(iii) ENNHRI

297. The ENNHRI also drew the Court's attention to international instruments such as the ICCPR, the American Convention on Human Rights, and the EU Charter of Fundamental Rights. It observed that in 2015

the Human Rights Committee reviewed the State Party report of the United Kingdom of Great Britain and Northern Ireland. It expressed concern that RIPA provided for untargeted warrants for the interception of external communications without affording the same safeguards as applied to internal communications, and it made a number of detailed recommendations, including the creation of sufficiently precise and foreseeable legal provisions, and judicial involvement in the authorisation of such measures.

(iv) The Helsinki Foundation for Human Rights ("HFHR")

298. The HFHR described their experience challenging the surveillance of communications by public authorities in Poland, which culminated in the Constitutional Tribunal finding certain aspects of the relevant legislation to be unconstitutional. The legislation was subsequently amended.

(v) The International Commission of Jurists ("ICJ")

299. The ICJ submitted that in light of the scale and scope of the interference with privacy entailed in mass surveillance, the distinction between the acquisition of metadata and content had become out-dated. Furthermore, the fact that, in a mass surveillance operation, elements of the interference with rights might take place outside a State's territorial jurisdiction didn't preclude that State's responsibility, since its control over the information was sufficient to establish jurisdiction.

(vi) Open Society Justice Initiative ("OSJI")

300. OSJI submitted that both the amount of data available for interception today and governments' appetite for data far exceeded what was possible in the past. Consequently, bulk interception was a particularly serious interference with privacy which could, through its "chilling effect", potentially interfere with other rights such as freedom of expression and freedom of association. To be lawful, bulk interception should therefore satisfy several preconditions: the governing law had to be sufficiently precise; the scope of the information gathered had to be limited by time and geography; and information should only be gathered based on "reasonable suspicion".

(vii) European Digital Rights ("EDRi") and other organisations active in the field of human rights in the information society

301. EDRi and others argued that the present case offered the Court a crucial opportunity to revise its framework for the protection of metadata. Governments had built their surveillance programmes based on the distinction drawn between content and metadata in *Malone v. the United Kingdom*, 2 August 1984, Series A no. 82, but at the time that case was decided neither the Internet nor mobile phones existed. Today, metadata

could paint a detailed and intimate picture of a person: it allowed for mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with. Moreover, the level of detail that could be gleaned was magnified when analysed on a large scale. Indeed, Stewart Baker, general counsel of the NSA, had indicated that metadata could disclose everything about someone's life, and that if you had enough metadata, you wouldn't need content. As a result, different degrees of protection should not be afforded to personal data based on the arbitrary and irrelevant distinction between content and metadata, but rather on the inferences that could be drawn from the data.

(viii) The Law Society of England and Wales

302. The Law Society expressed deep concern about the implications of the section 8(4) regime for the principle of legal professional privilege. In particular, the regime permitted the interception of legally privileged and confidential communications between lawyers and clients, even when both were in the United Kingdom. It also permitted the routine collection of metadata attaching to such communications. Furthermore, once intercepted these legally privileged communications could be used, provided that the primary purpose and object of the warrant was the collection of external communications. This arrangement – and the absence of adequate constraints on the use of such material – was apt to have a potentially severe chilling effect on the frankness and openness of lawyer-client communications.

(c) The Court's assessment

(i) General principles relating to secret measures of surveillance, including the interception of communications

303. Although the Court has developed extensive jurisprudence on secret measures of surveillance, its case-law concerns many different forms of surveillance, including, but not limited to, the interception of communications. It also concerns many different forms of "interference" with applicants' right to respect for their private lives; for example, while some cases concern the interception of the content of communications, others concern the interception or obtaining of communications data, or the tracking of individuals via GPS. As the Court has at times differentiated between the different types of surveillance and the different forms of interference, there is no one set of general principles which apply in all cases concerning secret measures of surveillance. The following principles can, however, be extrapolated from the Court's case-law.

304. Any interference with an individual's Article 8 rights can only be justified under Article 8 § 2 if it is in accordance with the law, pursues one

or more of the legitimate aims to which that paragraph refers and is necessary in a democratic society in order to achieve any such aim (see *Roman Zakharov*, cited above, § 227, and *Kennedy*, cited above, § 130).

305. According to the Court's well established case-law, the wording "in accordance with the law" requires the impugned measure to have some basis in domestic law (as opposed to a practice which does not have a specific legal basis – see *Heglas v. the Czech Republic*, no. 5935/02, § 74, 1 March 2007). It must also be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must therefore be accessible to the person concerned and foreseeable as to its effects (see *Roman Zakharov*, cited above, § 228; see also, among many other authorities, *Rotaru v. Romania* [GC], no. 28341/95, § 52, ECHR 2000‑V; *S. and Marper*, cited above, § 95, and *Kennedy*, cited above, § 151).

306. The Court has held on several occasions that the reference to "foreseeability" in the context of secret surveillance cannot be the same as in many other fields. Foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to resort to such measures so that he can adapt his conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on secret surveillance measures, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (see *Roman Zakharov*, cited above, § 229; see also *Malone*, cited above, § 67, *Leander*, cited above, § 51; *Huvig v. France*, 24 April 1990, § 29, Series A no. 176‑B; *Valenzuela Contreras v. Spain*, 30 July 1998, § 46, Reports of Judgments and Decisions 1998‑V; *Rotaru*, cited above, § 55; *Weber and Saravia*, cited above, § 93; *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, § 75, 28 June 2007). Moreover, the law must indicate the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see *Roman Zakharov*, cited above, § 230; see also, among other authorities, *Malone*, cited above, § 68; *Leander*, cited above, § 51; *Huvig*, cited above, § 29; and *Weber and Saravia*, cited above, § 94).

307. In its case-law on the interception of communications in criminal investigations, the Court has developed the following minimum requirements that should be set out in law in order to avoid abuses of power: the nature of offences which may give rise to an interception order; a

definition of the categories of people liable to have their communications intercepted; a limit on the duration of interception; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which intercepted data may or must be erased or destroyed (see *Huvig*, cited above, § 34; *Valenzuela Contreras*, cited above, § 46; *Weber and Saravia*, cited above, § 95; and *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 76). In *Roman Zakharov* (cited above, § 231) the Court confirmed that the same six minimum requirements also applied in cases where the interception was for reasons of national security; however, in determining whether the impugned legislation was in breach of Article 8, it also had regard to the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law (*Roman Zakharov*, cited above, § 238).

308. As to the question whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, the Court has acknowledged that, when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. However, this margin is subject to European supervision embracing both legislation and decisions applying it. In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" to what is "necessary in a democratic society" (see *Roman Zakharov*, cited above, § 232; see also *Klass and Others v. Germany*, 6 September 1978, §§ 49, 50 and 59, Series A no. 28, *Weber and Saravia*, cited above, § 106 and *Kennedy*, cited above, §§ 153 and 154).

309. Review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will

necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure (see *Roman Zakharov*, cited above, § 233; see also *Klass and Others*, cited above, §§ 55 and 56).

310. As regards the third stage, after the surveillance has been terminated, the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers. There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively (see *Roman Zakharov*, cited above, § 234; see also *Klass and Others*, cited above, § 57, and *Weber and Saravia*, cited above, § 135) or, in the alternative, unless any person who suspects that he or she has been subject to surveillance can apply to courts, whose jurisdiction does not depend on notification to the surveillance subject of the measures taken (see *Roman Zakharov*, cited above, § 234; see also *Kennedy*, cited above, § 167).

(ii) Existing case-law on the bulk interception of communications

311. The Court has considered the Convention compatibility of regimes which expressly permit the bulk interception of communications on two occasions: first in *Weber and Saravia* (cited above), and then in *Liberty and Others v. the United Kingdom*, no. 58243/00, 1 July 2008.

312. In *Weber and Saravia* the applicants complained about the process of strategic monitoring under the amended G10 Act, which authorised the monitoring of international wireless telecommunications. Signals emitted from foreign countries were monitored by interception sites situated on German soil with the aid of certain catchwords which were listed in the monitoring order. Only communications containing these catchwords were recorded and used. Having particular regard to the six "minimum requirements" set out in paragraph 307 above, the Court considered that there existed adequate and effective guarantees against abuses of the State's strategic monitoring powers. It therefore declared the applicants' Article 8 complaints to be manifestly ill-founded.

313. In *Liberty and Others* the Court was considering the regime under section 3(2) of the Interception of Communications Act 1985, which was in effect the predecessor of the regime under section 8(4) of RIPA.

Section 3(2) allowed the executive to intercept communications passing between the United Kingdom and an external receiver. At the time of issuing a section 3(2) warrant, the Secretary of State was required to issue a certificate containing a description of the intercepted material which he considered should be examined. The 1985 Act provided that material could be contained in a certificate, and thus listened to or read, if the Secretary of State considered that this was required in the interests of national security, the prevention of serious crime or the protection of the United Kingdom's economy. However, external communications emanating from a particular address in the United Kingdom could only be included in a certificate for examination if the Secretary of State considered it necessary for the prevention or detection of acts of terrorism. The Court held that the domestic law at the relevant time (which predated the adoption of the Interception of Communications Code of Practice – see, in particular, paragraph 109 above) did not indicate with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. In particular, it did not set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material.

(iii) The test to be applied in the present case

314. The Court has expressly recognised that the national authorities enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security (see *Weber and Saravia*, cited above, § 106). Furthermore, in *Weber and Saravia* and *Liberty and Others* the Court accepted that bulk interception regimes did not *per se* fall outside this margin. Although both of these cases are now more than ten years old, given the reasoning of the Court in those judgments and in view of the current threats facing many Contracting States (including the scourge of global terrorism and other serious crime, such as drug trafficking, human trafficking, the sexual exploitation of children and cybercrime), advancements in technology which have made it easier for terrorists and criminals to evade detection on the Internet, and the unpredictability of the routes via which electronic communications are transmitted, the Court considers that the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States' margin of appreciation.

315. Nevertheless, as indicated previously, it is evident from the Court's case-law over several decades that all interception regimes (both bulk and targeted) have the potential to be abused, especially where the true breadth of the authorities' discretion to intercept cannot be discerned from the relevant legislation (see, for example, *Roman Zakharov*, cited above, and

Szabó and Vissy v. Hungary, no. 37138/14, 12 January 2016). Therefore, while States enjoy a wide margin of appreciation in deciding what type of interception regime is necessary to protect national security, the discretion afforded to them in operating an interception regime must necessarily be narrower. In this regard, the Court has identified six minimum requirements that both bulk interception and other interception regimes must satisfy in order to be sufficiently foreseeable to minimise the risk of abuses of power (see paragraph 307 above).

316. The applicants argue that in the present case the Court should "update" those requirements by including requirements for objective evidence of reasonable suspicion in relation to the persons for whom data is being sought, prior independent judicial authorisation of interception warrants, and the subsequent notification of the surveillance subject (see paragraph 280 above). In their view, such changes would reflect the fact that due to recent technological developments the interception of communications now has greater potential than ever before to paint an intimate and detailed portrait of a person's private life and behaviour. However, while the Court does not doubt the impact of modern technology on the intrusiveness of interception, and has indeed emphasised this point in its case-law, it would be wrong automatically to assume that bulk interception constitutes a greater intrusion into the private life of an individual than targeted interception, which by its very nature is more likely to result in the acquisition and examination of a large volume of his or her communications. In any event, although the Court would agree that the additional requirements proposed by the applicants might constitute important safeguards in some cases, for the reasons set out below it does not consider it appropriate to add them to the list of minimum requirements in the case at hand.

317. First of all, requiring objective evidence of reasonable suspicion in relation to the persons for whom data is being sought and the subsequent notification of the surveillance subject would be inconsistent with the Court's acknowledgment that the operation of a bulk interception regime in principle falls within a State's margin of appreciation. Bulk interception is by definition untargeted, and to require "reasonable suspicion" would render the operation of such a scheme impossible. Similarly, the requirement of "subsequent notification" assumes the existence of clearly defined surveillance targets, which is simply not the case in a bulk interception regime.

318. Judicial authorisation, by contrast, is not inherently incompatible with the effective functioning of bulk interception. Nevertheless, as the Venice Commission acknowledged in their report on the Democratic Oversight of Signals Intelligence Agencies (see paragraph 212 above), while the Court has recognised that judicial authorisation is an "important safeguard against arbitrariness" (see *Roman Zakharov*, cited above, § 249),

to date it has not considered it to be a "necessary requirement" or the exclusion of judicial control to be outside "the limits of what may be deemed necessary in a democratic society" (see, for example, *Roman Zakharov*, cited above, § 258; see also *Klass and Others*, cited above, §§ 51 and 56; *Weber and Saravia*, cited above, § 115; *Kennedy*, cited above, § 167; and *Szabó and Vissy,* cited above, § 77*)*. There would appear to be good reason for this. The Court has found it "desirable to entrust supervisory jurisdiction to a judge" because, as a result of the secret nature of the surveillance, the individual will usually be unable to seek a remedy of his or her own accord (see *Roman Zakharov*, cited above, § 233). However, that is not the case in every contracting State. In the United Kingdom, for example, any person who thinks that he or she has been subject to secret surveillance can lodge a complaint with the IPT (see paragraph 250 above). Consequently, in *Kennedy* the Court accepted that regardless of the absence of prior judicial authorisation, the existence of independent oversight by the IPT and the Interception of Communications Commissioner provided adequate safeguards against abuse (see *Kennedy*, cited above, §§ 167-169). In this regard, the Venice Commission also noted that independent oversight may be able to compensate for an absence of judicial authorisation (see paragraph 212 above).

319. Secondly, the Court has acknowledged that "the possibility of improper action by a dishonest, negligent or over-zealous official can never be completely ruled out whatever the system" (see *Klass and Others*, cited above, § 59), and one need only look at its most recent jurisprudence to find examples of cases where prior judicial authorisation provided limited or no protection against abuse. For example, in *Roman Zakharov*, any interception of communications had to be authorised by a court and the judge had to give reasons for the decision to authorise interceptions. However, as judicial scrutiny was limited in scope and the police had the technical means to circumvent the authorisation procedure and to intercept any communications without obtaining prior judicial authorisation, the Court found that Russian law was incapable of keeping the "interference" to what was "necessary in a democratic society". Similarly, in *Association for European Integration and Human Rights and Ekimdzhiev* the relevant law required judicial authorisation before interception could take place. Nevertheless, the Court found that numerous abuses had taken place (according to a recent report, more than 10,000 warrants were issued over a period of some twenty‑four months). More recently, in *Mustafa Sezgin Tanrıkulu v. Turkey*, no. 27473/06, § 64, 18 July 2017 the Court found a violation of Article 8 where an assize court had granted the National Intelligence Agency permission to intercept all domestic and international communications for a month and a half with a view to identifying terrorist suspects.

320. Therefore, while the Court considers judicial authorisation to be an important safeguard, and perhaps even "best practice", by itself it can neither be necessary nor sufficient to ensure compliance with Article 8 of the Convention (see *Klass and Others*, cited above, § 56). Rather, regard must be had to the actual operation of the system of interception, including the checks and balances on the exercise of power, and the existence or absence of any evidence of actual abuse (see *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 92). Accordingly, the Court will examine the justification for any interference in the present case by reference to the six minimum requirements, adapting them where necessary to reflect the operation of a bulk interception regime. It will also have regard to the additional relevant factors which it identified in *Roman Zakharov*, but did not classify as "minimum requirements"; namely, the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law (see paragraph 307 above).

(α) The existence of an interference

321. The Government do not dispute that there has been an interference with the applicants' Article 8 rights.

(β) Justification for the interference

322. As already noted, an interference can only be justified under Article 8 § 2 if it is in accordance with the law, pursues one or more legitimate aims and is necessary in a democratic society in order to achieve any such aim (see paragraph 303 above). In cases where the legislation permitting secret surveillance is contested before the Court, the lawfulness of the interference is closely related to the question whether the "necessity" test has been complied with and it is therefore appropriate for the Court to address jointly the "in accordance with the law" and "necessity" requirements (see *Roman Zakharov*, cited above, § 236 and *Kennedy*, cited above, § 155). The "quality of law" in this sense implies that the domestic law must not only be accessible and foreseeable in its application, but it must also ensure that secret surveillance measures are applied only when "necessary in a democratic society", in particular by providing for adequate and effective safeguards and guarantees against abuse.

323. The parties do not dispute that the section 8(4) regime had a basis in domestic law; nor do they dispute that the regime pursued the legitimate aims of the protection of national security, the prevention of crime and the protection of the economic well-being of the country. The applicants do, however, contest the quality of domestic law and, in particular, its accessibility and foreseeability.

324. The Court will therefore assess in turn the accessibility of the domestic law, followed by its foreseeability and necessity, having regard to

the six minimum requirements established in its case law, before turning its attention to the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law (see paragraph 307 above).

- *Accessibility*

325. The applicants challenge the accessibility of domestic law on the grounds that it is too complex to be accessible to the public, and it relies on "below the waterline" arrangements. It is true that most of the reports into the United Kingdom's secret surveillance regimes have criticised the piecemeal development – and subsequent lack of clarity – of the legal framework (see paragraphs 152, 162 and 167 above). However, as with other cases in which domestic law has been considered *in abstracto* and amendments have been made to the legislation while the application was pending (see, for example, *Association for European Integration and Human Rights and Ekimdzhiev*), in the present case the Court must review the Convention compliance of the law in force at the date of its examination of the applicants' complaints. It therefore can, and should, take into account the IC Code which was amended in 2016 to clarify the legal framework and reflect the further disclosures which were made following the Snowden revelations and which are examined in detail in the ISC report, the Anderson report and the ISR report (see paragraphs 90, 148-150, 160-165 and 166-172 above). As the IC Code is a public document, subject to the approval of both Houses of Parliament, and has to be taken into account both by those exercising interception duties and by courts and tribunals, the Court has expressly accepted that its provisions could be taken into consideration in assessing the foreseeability of the RIPA regime (see *Kennedy*, cited above, § 157).

326. Insofar as the applicants complain about the existence of "below the waterline" arrangements, the Court has acknowledged that States do not have to make public all the details of the operation of a secret surveillance regime, provided that sufficient information is available in the public domain (see *Roman Zakharov*, cited above, §§ 243-244 and 247; see also, among many examples, *Szabó and Vissy,* cited above, § 64, and *Kennedy*, cited above, § 159). In the context of secret surveillance, it is inevitable that "below the waterline" arrangements will exist, and the real question for the Court is whether it can be satisfied, based on the "above the waterline" material, that the law is sufficiently foreseeable to minimise the risk of abuses of power. This is a question that goes to the foreseeability and necessity of the relevant law, rather than its accessibility.

327. Therefore, while the Court concurs with several of the aforementioned domestic reports that RIPA and the accompanying surveillance framework are extremely complex, in the present case it will concentrate on the requirements of "foreseeability" and "necessity".

- *The scope of application of secret surveillance measures*

328. The first two minimum requirements have traditionally been referred to as the nature of the offences which might give rise to an interception order and a definition of the categories of people liable to have their telephones tapped. In *Roman Zakharov* the Court made clear that pursuant to these two requirements "the national law must define the scope of application of secret surveillance measures by giving citizens an adequate indication as to the circumstances in which public authorities are empowered to resort to such measures" (see *Roman Zakharov*, cited above, §§ 243).

329. In a targeted interception regime, the nature of the communications to be intercepted should be tightly defined, but once interception takes place it is likely that all – or nearly all – of the intercepted communications are analysed. The opposite will normally be true of a bulk interception regime, where the discretion to intercept is broader, but stricter controls will be applied at the selection for examination stage. In fact, in the present case, it is clear from Chapter 6 of the IC Code (see paragraph 90 above), the ISC report (see paragraphs 151-159 above), the first IPT judgment in the *Liberty* proceedings (see paragraphs 41-49 above) and the Government's observations that there are four distinct stages to the section 8(4) regime:

1. The interception of a small percentage of Internet bearers, selected as being those most likely to carry external communications of intelligence value.

2. The filtering and automatic discarding (in near real-time) of a significant percentage of intercepted communications, being the traffic least likely to be of intelligence value.

3. The application of simple and complex search criteria (by computer) to the remaining communications, with those that match the relevant selectors being retained and those that do not being discarded.

4. The examination of some (if not all) of the retained material by an analyst).

330. Thus, in addressing the first two minimum requirements, the Court will examine first, whether the grounds upon which a warrant can be issued are sufficiently clear; secondly, whether domestic law gives citizens an adequate indication of the circumstances in which their communications might be intercepted; and thirdly, whether domestic law gives citizens an adequate indication of the circumstances in which their communications might be selected for examination (see paragraph 328 above).

331. According to RIPA and the IC Code, the Secretary of State can only issue a warrant if he is satisfied that it is necessary in the interests of national security, for the purpose of preventing or detecting serious crime, or for the purpose of safeguarding the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security; and that the conduct authorised by the warrant is

proportionate to what is sought to be achieved by that conduct. Pursuant to domestic law, when assessing necessity and proportionality, account should be taken of whether the information sought under the warrant could reasonably be obtained by other means (section 5(3) of RIPA and Chapter 6 of the IC Code – see paragraphs 57 and 90 above). It is clear that insofar as RIPA and the IC Code use the terms "necessity" and "proportionality" they are intended to ensure compliance with the requirements of Articles 8 and 10 of the Convention and should therefore be understood in the Convention sense (see paragraph 3.5 of the IC Code, at paragraph 90 above).

332. The Court has held that the condition of foreseeability does not require States to set out exhaustively by name the specific offences which may give rise to interception, provided that there is sufficient detail about the nature of the offences in question (see *Roman Zakharov*, cited above, §§ 243-244; see also, among many examples, *Szabó and Vissy,* cited above, § 64, and *Kennedy*, cited above, § 159). Moreover, the Court has expressly recognised the need to avoid excessive rigidity in the wording of certain statures and to keep pace with changing circumstances (see *Szabó and Vissy,* cited above, § 64 and *Kokkinakis v. Greece*, 25 May 1993, § 40, Series A no. 260-A).

333. In *Kennedy* the Court had to consider whether the section 5(3) grounds (which apply to both section 8(1) and section 8(4) warrants) provided sufficient detail about the nature of the offences that might give rise to an interception order. It found that the term "national security" was frequently employed in both national and international legislation and constituted one of the legitimate aims to which Article 8 § 2 referred. It further noted that threats to national security tended to vary in character and might be unanticipated or difficult to define in advance. Finally, the Interception of Communications Commissioner had clarified that in practice "national security" allowed surveillance of activities which threatened the safety or well-being of the State and activities which were intended to undermine or overthrow Parliamentary democracy by political, industrial or violent means. It therefore found the term to be sufficiently clear (see *Kennedy*, cited above, § 159).

334. Furthermore, the Court observes that "serious crime" is clearly defined in section 81 of RIPA (see paragraphs 58-59 above; see also *Kennedy*, cited above, § 159) and the IC Code has clarified that the purpose of safeguarding the economic well-being of the United Kingdom is restricted to those interests which are also relevant to the interests of national security (see paragraph 90 above).

335. The Court therefore considers that section 5(3) is sufficiently clear, giving citizens an adequate indication of the circumstances in which and the conditions on which a section 8(4) warrant might be issued.

336. As for the persons liable to have their communications intercepted, it is clear that this category is wide. Section 8(4) only permits the Secretary

of State to issue a warrant for the interception of external communications, which in principle excludes communications where both of the parties are in the British Islands. Although there has been some confusion about the application of the terms "external communications" and "internal communications" to modern forms of communications, the Secretary of State for the Foreign and Commonwealth, in giving evidence to the Intelligence and Security Committee of Parliament in October 2014, provided clarification about the status of emails, web-browsing, social media and cloud storage (see paragraph 71 above). However, even where it is clear that a communication is "internal", as it is between two people in the British Islands, in practice, some or all of its parts might be routed through one or more other countries, and would therefore be at risk of being intercepted under the section 8(4) regime. This is expressly permitted by section 5(6) of RIPA, which allows the interception of communications not identified in the warrant (see paragraph 63 above).

337. That being said, it is clear that the targeted bearers are not chosen at random. They are selected because they are believed to be the most likely to carry external communications of intelligence interest (paragraph 6.7 of the IC Code, at paragraph 90 above and the Annual Report of the Interception of Communications Commissioner for 2016, at paragraph 178 above). Therefore, while anyone could potentially have their communications intercepted under the section 8(4) regime, it is clear that the intelligence services are neither intercepting everyone's communications, nor exercising an unfettered discretion to intercept whatever communications they wish. In practice, one of the grounds set out in section 5(3) of RIPA must be satisfied, bulk interception must be proportionate to the aim sought to be achieved, and – at least at the macro level of selecting the bearers for interception – only external communications can be targeted.

338. As the ISC observed, it would be desirable for the criteria for selecting the bearers to be subject to greater oversight by the Commissioner (see paragraph 157 above). However, the Court has already noted that by its very nature a bulk interception regime will allow the authorities a broad discretion to intercept communications and, as such, it does not consider this fact alone to be fatal to the Article 8 compliance of the section 8(4) regime. While the discretion to intercept should not be unfettered – since the interception and filtering of a communication, even if it is subsequently discarded in near real-time, is sufficient to constitute an interference with a persons' rights under Article 8 of the Convention –, more rigorous safeguards will be required at the third and fourth stages identified in paragraph 329 above, as any interference in such cases will be significantly greater.

339. With regard to the selection of communications for examination, once communications are intercepted and filtered, those not discarded in near real-time are further searched; in the first instance by the automatic

application, by computer, of simple selectors (such as email addresses or telephone numbers) and initial search criteria, and subsequently by the use of complex searches (see paragraph 6.4 of the IC Code at paragraph 90; see also the ISC report at paragraphs 151-159 above and the Government's observations in the present case). In *Liberty and Others*, the Court compared the predecessor of the section 8(4) regime unfavourably with the German system under consideration in *Weber and Saravia*, noting that the G10 Act authorised the Federal Intelligence Service to carry out monitoring of communications only with the aid of search terms which served, and were suitable for, the investigation of the dangers described in the monitoring order and which search terms had to be listed in the monitoring order (*Liberty and Others*, cited above, § 68 and *Weber and Saravia*, cited above, § 32).

340. This does not mean that selectors and search criteria need to be made public; nor does it mean that they necessarily need to be listed in the warrant ordering interception. In fact, in the *Liberty* proceedings the IPT found that the inclusion of the selectors in the warrant or accompanying certificate would "unnecessarily undermine and limit the operation of the warrant and be in any event entirely unrealistic" (see paragraph 44 above). The Court has no reason to call this conclusion into question. Nevertheless, the search criteria and selectors used to filter intercepted communications should be subject to independent oversight; a safeguard which appears to be absent in the section 8(4) regime. Indeed, the ISC report criticised the absence of any meaningful oversight of both the selectors and search criteria (see paragraph 157 above).

341. As a result of the application of selectors and automated searches, an index is generated. Material not on the index is discarded. Only material on the index may be examined by an analyst, and only if it satisfies the two criteria in section 16 of RIPA, namely certification by the Secretary of State as to necessity (section 16(1); see paragraphs 78-85 above) and presence for the time being in the British Islands (section 16(2)).

342. As regards the certification by the Secretary of State, the ISC observed that the categories set out in the certificates were set out in very general terms (for example, "material providing intelligence on terrorism (as defined by the Terrorism Act 2000 (as amended)) including, but not limited to, terrorist organisations, terrorists, active sympathisers, attack planning, fund-raising") (see paragraph 156 above). Similarly, the Independent Reviewer of Terrorism Legislation recommended that the purposes for which material or data was sought should be spelled out by reference to specific operations or mission purposes (for example, "attack planning by ISIL in Iraq/Syria against the UK") (see paragraph 162 above). In order for this safeguard to be effective, the Court agrees that it would be highly desirable for the certificate to be expressed in more specific terms than it currently appears to be.

343. On the other hand, the exclusion of communications of individuals known currently to be in the British Islands is, in the opinion of the Court, an important safeguard, since persons of interest to the intelligence services who are known to be in the British Islands could be subject to a targeted warrant under section 8(1) of RIPA. The intelligence services should not be permitted to obtain via a bulk warrant what they could obtain via a targeted warrant.

344. According to paragraph 7.18 of the IC Code, periodic audits should be carried out to ensure that the requirements set out in section 16 of RIPA are being met and any breaches of safeguards should be notified to the Interception of Communications Commissioner (see paragraph 90 above). In his 2016 annual report, echoing comments also made in his 2014 and 2015 reports, the Commissioner observed that the process by which analysts selected material for examination, which did not require pre-authorisation by a more senior operational manager, relied mainly on the professional judgment of analysts, their training and subsequent management oversight (see paragraph 179 above).

345. On balance, the Court agrees that it would be preferable for the selection of material by analysts to be subject at the very least to pre-authorisation by a senior operational manager. However, given that analysts are carefully trained and vetted, records are kept and those records are subject to independent oversight and audit (see paragraph 7.15 and 7.18 of the IC Code, at paragraph 90 above), the absence of pre-authorisation would not, in and of itself, amount to a failure to provide adequate safeguards against abuse.

346. Nevertheless, the Court must have regard to the operation of the section 8(4) regime as a whole, and in particular the fact that the list from which analysts are selecting material is itself generated by the application of selectors and selection criteria which were not subject to any independent oversight. In practice, therefore, the only independent oversight of the process of filtering and selecting intercept data for examination is the *post factum* audit by the Interception of Communications Commissioner and, should an application be made to it, the IPT. In *Kennedy* the Court held that the RIPA procedure for examining intercept material was sufficiently clear. That finding, however, was expressly based on the fact that unlike the regime examined in *Liberty and Others*, which concerned the indiscriminate capturing of data, that case was concerned with an interception warrant for one set of premises only; a fact which in and of itself limited the scope of the authorities' discretion to intercept and listen to private communications (see *Kennedy*, cited above, § 162). In a bulk interception regime, where the discretion to intercept is not significantly curtailed by the terms of the warrant, the safeguards applicable at the filtering and selecting for examination stage must necessarily be more robust.

347. Therefore, while there is no evidence to suggest that the intelligence services are abusing their powers – on the contrary, the Interception of Communications Commissioner observed that the selection procedure was carefully and conscientiously undertaken by analysts (see paragraph 179 above) –, the Court is not persuaded that the safeguards governing the selection of bearers for interception and the selection of intercepted material for examination are sufficiently robust to provide adequate guarantees against abuse. Of greatest concern, however, is the absence of robust independent oversight of the selectors and search criteria used to filter intercepted communications.

- The exemption of related communications data from the safeguards applicable to the searching and examining of content

348. The Article 8(4) regime permits the bulk interception of both content and related communications data (the latter being the "who, when and where" of a communication). However, section 16 applies only to "intercepted material" which, according to the interpretation provision in section 20 of RIPA, is defined as the content of intercepted communications (see paragraph 78 above). The related communications data of all intercepted communications – even internal communications incidentally intercepted as a "by-catch" of a section 8(4) warrant – can therefore be searched and selected for examination without restriction.

349. The Government contend that access to communications data is necessary to give effect to one of the section 16 safeguards, namely to determine whether a person is or is not in the British Islands. They further contend that as communications data is less intrusive than data relating to content (at least when compared on a like-for-like basis), its interception, storage and use should not be subject to the same six minimum requirements (see paragraph 307 above). Instead, the Court should simply ask whether the law was sufficiently clear to give the individual adequate protection against arbitrary interference.

350. The Court has distinguished between different methods of investigation which result in different levels of intrusion into an individual's private life. According to the Court, the interception of communications represents one of the gravest intrusions, as it is capable of disclosing more information on a person's conduct, opinions or feelings (see *Uzun v. Germany*, no. 35623/05, § 52, ECHR 2010 (extracts))). Consequently, in *Uzun* the Court found that the interception of communications represented a greater intrusion into an individual's private life than the tracking of his vehicle via GPS (see *Uzun*, cited above, § 52). In *Ben Faiza v. France*, no. 31446/12, 8 February 2018, it further distinguished between the tracking of a vehicle, which nevertheless made it possible to geolocate a person in real time, and the lower level of intrusion occasioned by the transmission to

a judicial authority of existing data held by a public or private body (see *Ben Faiza*, cited above, § 74).

351. However, thus far the Court has only declined to apply the minimum requirements test in secret surveillance cases which did not involve the interception of communications, and in which the degree of intrusion was not considered to be comparable to that caused by interception (see for example, *R.E. v. the United Kingdom*, no. 62498/11, 27 October 2015 and *Uzun*, cited above).

352. In any event, it is not necessary for the Court to decide whether the six minimum requirements apply to the interception of communications data since, save for the section 16 safeguards, the section 8(4) regime treats intercepted content and related communications data in the same way. It will therefore focus its attention on whether the justification provided by the Government for exempting related communications data from this safeguard is proportionate to the legitimate aim pursued; that is, ensuring the effectiveness of that safeguard in respect of content.

353. It is not in doubt that communications data is a valuable resource for the intelligence services. It can be analysed quickly to find patterns that reflect particular online behaviours associated with activities such as a terrorist attack and to illuminate the networks and associations of persons involved in such attacks, making it invaluable in fast-moving operations; and, unlike much data relating to content, it is not generally encrypted (see paragraphs 158, 163, 169, 176 and 301 above).

354. Furthermore, the Court accepts that the effectiveness of the section 16(2) safeguard depends on the intelligence services having a means of determining whether a person is in the British Islands, and access to related communications data would provide them with that means.

355. Nevertheless, it is a matter of some concern that the intelligence services can search and examine "related communications data" apparently without restriction. While such data is not to be confused with the much broader category of "communications data", it still represents a significant quantity of data. The Government confirmed at the hearing that "related communications data" obtained under the section 8(4) regime will only ever be traffic data. However, according to paragraphs 2.24-2.27 of the ACD Code (see paragraph 117 above), traffic data includes information identifying the location of equipment when a communication is, has been or may be made or received (such as the location of a mobile phone); information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication; routing information identifying equipment through which a communication is or has been transmitted (for example, dynamic IP address allocation, file transfer logs and e-mail headers (other than the subject line of an e-mail, which is classified as content)); web browsing information to the extent that only a host machine, server, domain name or IP address is disclosed (in

other words, website addresses and Uniform Resource Locators ("URLs") up to the first slash are communications data, but after the first slash content); records of correspondence checks comprising details of traffic data from postal items in transmission to a specific address, and online tracking of communications (including postal items and parcels) (see paragraph 117 above).

356. In addition, the Court is not persuaded that the acquisition of related communications data is necessarily less intrusive than the acquisition of content. For example, the content of an electronic communication might be encrypted and, even if it were decrypted, might not reveal anything of note about the sender or recipient. The related communications data, on the other hand, could reveal the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. In bulk, the degree of intrusion is magnified, since the patterns that will emerge could be capable of painting an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with (see paragraph 301 above).

357. Consequently, while the Court does not doubt that related communications data is an essential tool for the intelligence services in the fight against terrorism and serious crime, it does not consider that the authorities have struck a fair balance between the competing public and private interests by exempting it in its entirety from the safeguards applicable to the searching and examining of content. While the Court does not suggest that related communications data should only be accessible for the purposes of determining whether or not an individual is in the British Islands, since to do so would be to require the application of stricter standards to related communications data than apply to content, there should nevertheless be sufficient safeguards in place to ensure that the exemption of related communications data from the requirements of section 16 of RIPA is limited to the extent necessary to determine whether an individual is, for the time being, in the British Islands.

- *Duration of the secret surveillance measure*

358. Pursuant to section 9 of RIPA (see paragraph 62 above), a section 8(4) warrant ceases to have effect at the end of the "relevant period" unless it is renewed. For warrants issued by the Secretary of State for reasons of national or economic security, the "relevant period" is six months, and for warrants issued by the Secretary of State for the purposes of preventing serious crime, the "relevant period" is three months. These warrants are renewable for periods of six and three months respectively. Warrants may be renewed at any point before their expiry date by application to the Secretary of State. The application must contain the same

information as the original application; it must also contain an assessment of the value of the interception to date and explain why the continuation of interception is necessary, within the meaning of section 5(3), and proportionate (see paragraph 6.22-6.24 of the IC Code at paragraph 90 above). Paragraph 6.7 of the IC Code requires regular surveys of relevant communications links (see paragraph 90 above). Consequently, any application for renewal of a warrant would have to show that interception of those links continued to be of value, and continued to be necessary and proportionate (in the Convention sense).

359. Furthermore, the Secretary of State must cancel a warrant if satisfied that it is no longer necessary on section 5(3) grounds (see section 9 of RIPA at paragraph 62 above).

360. In *Kennedy* (cited above, § 161) the Court considered the same provisions on the duration and renewal of interception warrants (in that case, in the context of the section 8(1) regime) and found that the rules were sufficiently clear as to provide adequate safeguards against abuse. In particular, it noted that the duty on the Secretary of State to cancel warrants which were no longer necessary meant, in practice, that the intelligence services had to keep their warrants under continuous review. In light of the foregoing considerations, the Court sees no grounds upon which to reach a different conclusion in the present case. In particular, it sees no evidence to substantiate the applicants' claim that once issued, section 8(4) warrants could continue indefinitely regardless of whether they continued to be necessary and proportionate.

- Procedure to be followed for storing, accessing, examining and using the intercepted data

361. As already noted, analysts may only examine material which appears on the automatically generated index. Prior to analysts being able to read, look at or listen to material on the index, they must make a record of why access to the material is necessary for one of the statutory purposes set out in section 5(3) of RIPA, and proportionate, having regard to whether the information could reasonably be obtained by less intrusive means (see section 16 of RIPA, at paragraph 79 above, and paragraph 7.15 of the IC Code, at paragraph 90 above). Pursuant to section 16(2), they cannot select material for examination using criteria that refer to the communications of individuals known currently to be in the British Islands (see paragraph 79 above). Paragraph 7.16 of the IC Code also requires the analyst to indicate any circumstances likely to give rise to a degree of collateral infringement of privacy, together with the measures taken to reduce the extent of that intrusion (see paragraph 90 above). Subsequent access by the analyst is limited to a defined period of time; although that period of time may be renewed, the record must be updated giving reasons for renewal (see paragraph 7.17 of the IC Code, at paragraph 90 above).

362. Paragraph 7.15 of the IC Code further requires that analysts examining intercepted material must be specially authorised to do so; must receive regular mandatory training regarding on the provisions of RIPA and specifically the operation of section 16 and the requirements of necessity and proportionality; and must be vetted (see paragraph 90 above). Furthermore, regular audits are carried out which must include checks to ensure that the records requesting access to material have been compiled correctly, and that the material requested falls within the matters certified by the Secretary of State (see paragraph 7.18 of RIPA, at paragraph 90 above).

363. With regard to the storage of intercepted material, paragraph 7.7 of the IC Code requires that prior to its destruction, it must be stored securely and must not be accessible to persons without the required level of security clearance (see paragraph 90 above).

364. In light of the foregoing, and subject to its conclusions at paragraph 347 and 357 above, the Court would accept that the provisions relating to the storing, accessing, examining and using intercepted data are sufficiently clear.

- Procedure to be followed for communicating the intercepted data to other parties

365. While material is being stored, section 15(2) of RIPA and paragraphs 7.2 of the IC Code require that the following are limited to the minimum necessary for the "authorised purposes": the number of persons to whom the material or data is disclosed or made available; the extent to which the material or data is disclosed or made available; the extent to which the material or data is copied; and the number of copies that are made (see paragraphs 72-77 and 90 above). Pursuant to section 15(4) and paragraph 7.2 of the IC Code, something is necessary for the authorised purposes if, and only if, it continues to be, or is likely to become, necessary for the purposes mentioned in section 5(3) of RIPA; for facilitating the carrying out of any of the interception functions of the Secretary of State; for facilitating the carrying out of any functions of the Interception of Communications Commissioner or of the IPT; to ensure that a person conducting a criminal prosecution has the information he needs to determine what is required of him by his duty to secure the fairness of the prosecution; or for the performance of any duty imposed on any person under public records legislation (see paragraphs 72-77 and 90 above).

366. Paragraph 7.3 of the IC Code prohibits disclosure to persons who have not been appropriately vetted and also by the need-to-know principle: intercepted material must not be disclosed to any person unless that person's duties, which must relate to one of the authorised purposes, are such that he or she needs to know about the intercepted material to carry out those duties (see paragraph 90 above). In the same way, only so much of the intercepted material may be disclosed as the recipient needs. Paragraph 7.3 applies

equally to disclosure to additional persons within an agency, and to disclosure outside the agency. Pursuant to paragraph 7.4, it also applies not just to the original interceptor, but also to anyone to whom the intercepted material is subsequently disclosed (see paragraph 90 above).

367. According to paragraph 7.5 of the IC Code, where intercepted material is disclosed to the authorities of a country or territory outside the United Kingdom, the agency must take reasonable steps to ensure that the authorities in question have and will maintain the necessary procedures to safeguard the intercepted material, and to ensure that it is disclosed, copied, distributed and retained only to the minimum extent necessary. The intercepted material must not be further disclosed to the authorities of a third country or territory unless explicitly agreed with the issuing agency, and must be returned to the issuing agency or securely destroyed when no longer needed (see paragraph 90 above).

368. The Court considered very similar provisions in *Kennedy*; although paragraph 7.5 is new, paragraphs 7.3, 7.4 and 7.6 in the 2016 IC Code are identical to paragraphs 6.4, 6.5 and 6.6 of the previous version. It was satisfied that the provisions on processing and communication of intercept material provided adequate safeguards for the protection of data obtained (see *Kennedy*, cited above, § 163). In the present case, however, the applicants have expressed concern about an aspect of the procedure which was not addressed in *Kennedy*; namely, the requirement that disclosure and copying be "limited to the minimum necessary for the 'authorised purposes'", when something might be considered "necessary" for an "authorised purpose" if it was "likely to become necessary". As "likely to become necessary" is not further defined in RIPA or the IC Code, or indeed anywhere else, it could in practice give the authorities a broad power to disclose and copy intercept material. Nevertheless, it is clear that even if disclosure or copying is "likely to become necessary" for an "authorised purpose", the material can still only be disclosed to a person with the appropriate level of security clearance, who has a "need to know". Furthermore, only so much of the intercept material as the individual needs to know is to be disclosed; where a summary of the material would suffice, then only a summary should be disclosed.

369. Therefore, while it would be desirable for the term "likely to become necessary" to be more clearly defined in either RIPA or the IC Code, the Court considers that, taken as a whole, section 15 of RIPA and Chapter 7 of the IC Code provide adequate safeguards for the protection of data obtained.

- The circumstances in which intercept material must be erased or destroyed

370. Section 15(3) of RIPA and paragraph 7.8 of the IC Code require that every copy of intercepted material or data (together with any extracts

and summaries) be destroyed securely as soon as retention is no longer necessary for any of the section 5(3) purposes (see paragraphs 74 and 90 above). In practice, this means that intercepted material which is filtered out in near real-time is destroyed. Similarly, following the application of selectors and search criteria, material which is not added to the analyst's index is also destroyed (see paragraphs 72-77 and 90 above).

371. Paragraph 7.9 provides that where an intelligence service receives unanalysed intercepted material and related communications data from interception under a section 8(4) warrant, it must specify maximum retention periods for different categories of the data which reflect its nature and intrusiveness. These specified periods should normally be no longer than two years, and should be agreed with the Interception of Communications Commissioner. So far as possible, all retention periods should be implemented by a process of automated deletion, which is triggered once the applicable maximum retention period has been reached for the data at issue (see paragraphs 72-77 above). Pursuant to paragraph 7.8, if intercepted material is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid under section 15(3) of RIPA (see paragraph 90 above).

372. According to the 2016 annual report of the Interception of Communications Commissioner, every interception agency had a different view on what constituted an appropriate retention period for intercepted material and related communications data. The retention periods for content ranged between thirty days and one year and the retention periods for related communications data ranged between six months and one year (see paragraph 186 above). Therefore, while the specific retention periods are not in the public domain, it is clear that they cannot exceed two years and, in practice, they do not exceed one year (with much content and related communications data being retained for significantly shorter periods).

373. Furthermore, where an application is lodged with the IPT, it can examine whether the time-limits for retention have been complied with and, if they have not, it may find that there has been a breach of Article 8 of the Convention and order the destruction of the relevant material. Where the retention has resulted in damage, detriment or prejudice, compensation may also be awarded. In the *Liberty* proceedings, brought by the applicants in the third of the joined cases, the IPT found that there had been a breach of Article 8 of the Convention by virtue of the fact that email communications of Amnesty International, which had been intercepted and accessed "lawfully and proportionately", had nevertheless been retained for longer than was permitted under GCHQ's internal policies. GCHQ was ordered to destroy the communications within seven days, and to provide a closed report within fourteen days confirming their destruction. A hard copy of the communications was to be delivered to the Commissioner (see paragraph 54 above).

374. Therefore, in the Court's view the provisions on the erasure and destruction of intercept material are also sufficiently clear.

- *Supervision, notification and remedies*

375. Supervision of the regime is carried out at a number of levels. First of all, according to the Interception of Communications Commissioner, a "critical quality assurance function [is] initially carried out by the staff and lawyers within the intercepting agency or the warrant-granting department" (see paragraph 180 above). The warrant-granting departments provide independent advice to the Secretary of State and perform important pre-authorisation scrutiny of warrant applications and renewals to ensure that they were (and remained) necessary and proportionate (see paragraph 180 above).

376. Secondly, section 8(4) warrants must be authorised by the Secretary of State. As already noted, while the Court has recognised judicial authorisation to be an "important safeguard against arbitrariness" (see *Roman Zakharov*, cited above, § 249), to date it has not considered it to be a "necessary requirement" (see, for example, *Roman Zakharov*, cited above, § 258; see also *Klass and Others*, cited above, § 51; *Weber and Saravia*, cited above, § 115; *Kennedy*, cited above, § 31; and *Szabó and Vissy,* cited above, § 77*)*. Although desirable in principle, by itself it is neither necessary nor sufficient to ensure compliance with Article 8 of the Convention (see paragraphs 318-320 above).

377. It is true that the Court has generally required a non-judicial authority to be sufficiently independent of the executive (see *Roman Zakharov*, cited above, § 258). However, it must principally have regard to the actual operation of a system of interception as a whole, including the checks and balances on the exercise of power, and the existence (or absence) of any evidence of actual abuse (see paragraph 320 above), such as the authorising of secret surveillance measures haphazardly, irregularly or without due and proper consideration (see *Roman Zakharov*, cited above, § 267).

378. In the present case there is no evidence to suggest that the Secretary of State was authorising warrants without due and proper consideration. The authorisation procedure was subject to independent oversight by the Interception of Communications Commissioner (recently replaced by the Investigatory Powers Commissioner following the coming into force of the Investigatory Powers Act 2016 – see paragraph 147 above), who was independent of the executive and the legislature, held or had held high judicial office, and was tasked with overseeing the general functioning of the surveillance regime and the authorisation of interception warrants in specific cases. The Commissioner reported annually to the Prime Minister and his report was a public document (subject to the non-disclosure of confidential annexes) which was laid before Parliament. In undertaking his

review of surveillance practices, he was granted access to all relevant documents, including closed materials, and all those involved in interception activities had a duty to disclose to him any material he required. The obligation on the intelligence services to keep records ensured that he had effective access to details of surveillance activities undertaken (see paragraph 145 above). In 2016, 970 warrants were examined during twenty-two interception inspections, representing 61% of the number of warrants in force at the end of the year and 32% of the total of new warrants issued in 2016 (see paragraph 185 above). As a consequence, in *Kennedy* the Court accepted that despite the fact that the section 8(1) warrant was authorised by the Secretary of State, sufficient independence was provided by the Interception of Communications Commissioner (see *Kennedy*, cited above, § 166).

379. Furthermore, the IPT has extensive jurisdiction to examine any complaint of unlawful interception: unlike in many other countries, its jurisdiction does not depend on notification of the interception to its subject (see paragraph 124 above), which means that any person who believes that he or she has been subject to secret surveillance may make an application to it (see paragraph 318 above). Its members must hold or have held high judicial office or be a qualified lawyer of at least ten years' standing (see paragraph 123 above). Those involved in the authorisation and execution of an intercept warrant are required to disclose to it all the documents it may require, including "below the waterline" documents which could not be made public for reasons of national security (see paragraph 127 above); it has discretion to hold oral hearings, in public, where possible (see paragraphs 131, 138 and 139 above); in closed proceedings it may appoint Counsel to the Tribunal also to make submissions on behalf of claimants who cannot be represented (see paragraph 142 above); and when it determines a complaint it has the power to award compensation and make any other order it sees fit, including quashing or cancelling any warrant and requiring the destruction of any records (see paragraph 128 above). The publication of the IPT's legal rulings further enhances the level of scrutiny afforded to secret surveillance activities in the United Kingdom (see *Kennedy*, cited above, § 167).

380. In any case, the Court notes that under the new Investigatory Powers Act 2016 warrants will have to be approved by judicial commissioners following their authorisation by the Secretary of State. Although this new procedure has not yet been implemented, the Investigatory Powers Commissioner and the deputy Investigatory Powers Commissioner have been appointed (see paragraph 197 above).

381. Therefore, while the Court considers judicial authorisation to be highly desirable and, in its absence, will generally require a non-judicial authority to be independent of the executive, in the present case, in view of the pre-authorisation scrutiny of warrant applications, the extensive post-

authorisation scrutiny provided by the (independent) Commissioner's office and the IPT, and the imminent changes to the impugned regime, it would accept that the authorisation of section 8(4) warrants by the Secretary of State does not, in and of itself, give rise to a breach of Article 8 of the Convention.

382. Finally, the Court recalls that in light of the Edward Snowden revelations, there were three thorough independent reviews of the existing interception regimes, and none of the reviewing bodies found any evidence that deliberate abuse of interception powers was taking place (see paragraphs 148-172 above).

383. In light of the above considerations, the Court is of the opinion that the supervision and oversight of the bulk interceptions capable of providing adequate and effective guarantees against abuse.

- *Proportionality*

384. With regard to the proportionality of the bulk interception regime, the Court notes that the Independent Reviewer of Terrorism Legislation, examined a great deal of closed material and concluded that bulk interception was an essential capability: first, because terrorists, criminals and hostile foreign intelligence services had become increasingly sophisticated at evading detection by traditional means; and secondly, because the nature of the global Internet meant that the route a particular communication would travel had become hugely unpredictable. Although he and his team (including a person with the necessary technical background to understand the systems and techniques used by GCHQ, and the uses to which they could be put, an investigator with experience as a user of secret intelligence, including intelligence generated by GCHQ, and senior independent counsel with the skills and experience to challenge forensically the evidence and the case studies presented by the security and intelligence services) looked at alternatives to bulk interception (including targeted interception, the use of human sources and commercial cyber-defence products), they concluded that no alternative or combination of alternatives would be sufficient to substitute for the bulk interception power (see paragraph 176 above).

385. Similarly, while acknowledging the risks that bulk interception can pose for individual rights, the Venice Commission nevertheless recognised its intrinsic value for security operations, since it enabled the security services to adopt a proactive approach, looking for hitherto unknown dangers rather than investigating known ones (see paragraph 211 above).

386. The Court sees no reason to disagree with the thorough examinations carried out by these bodies and the conclusions subsequently reached. It is clear that bulk interception is a valuable means to achieve the legitimate aims pursued, particularly given the current threat level from both global terrorism and serious crime.

(γ) Conclusions

387. In light of the foregoing considerations, the Court considers that the decision to operate a bulk interception regime was one which fell within the wide margin of appreciation afforded to the Contracting State. Furthermore, in view of the independent oversight provided by the Interception of Communications Commissioner and the IPT, and the extensive independent investigations which followed the Edward Snowden revelations, it is satisfied that the intelligence services of the United Kingdom take their Convention obligations seriously and are not abusing their powers under section 8(4) of RIPA. Nevertheless, an examination of those powers has identified two principal areas of concern; first, the lack of oversight of the entire selection process, including the selection of bearers for interception, the selectors and search criteria for filtering intercepted communications, and the selection of material for examination by an analyst; and secondly, the absence of any real safeguards applicable to the selection of related communications data for examination.

388. In view of these shortcomings and to the extent just outlined, the Court finds that the section 8(4) regime does not meet the "quality of law" requirement and is incapable of keeping the "interference" to what is "necessary in a democratic society". There has accordingly been a violation of Article 8 of the Convention.

B. The intelligence sharing regime

389. The applicants in the third of the joined cases complain that the respondent State's receipt of material intercepted by the NSA under PRISM and Upstream was in breach of their rights under Article 8 of the Convention. The applicants in the first of the joined cases complain more generally about the receipt of information from foreign intelligence services.

1. Admissibility

(a) The parties' submissions

390. The Government argued that the applicants could not claim to be victims of the alleged violation within the meaning of Article 34 of the Convention since they could not possibly have been affected by the intelligence sharing regime. They did not contend, and had put forward no evidential basis for contending, that their communications had in fact been intercepted under PRISM/Upstream and subsequently shared with the United Kingdom intelligence services. Rather, they asserted only that their communications "might have been" subject to foreign interception conveyed to United Kingdom authorities, or that they "believed" that to be the case. As such, their complaint was an abstract one about the regime

itself, and the Court should not entertain an abstract challenge when the applicants had available to them an effective remedy in the form of the IPT.

391. The applicants, on the other hand, submitted that on account of their global public interest activities and the very broad range of persons and organisations with which they were in contact, they were at genuine risk of having their communications obtained by a foreign intelligence service and requested by the United Kingdom authorities. They further submitted that there was no adequate remedy available under domestic law for the alleged breach of their Convention rights.

(b) The Court's assessment

392. The Court has accepted that an applicant could claim to be the victim of a violation occasioned by the mere existence of secret surveillance measures, or legislation permitting secret surveillance measures, if the following conditions were satisfied: first, the Court would examine whether the applicant could possibly be affected by the legislation permitting secret surveillance measures; and secondly, it would take into account the availability of remedies at the national level and adjust the degree of scrutiny depending on the effectiveness of such remedies. Where the domestic system did not afford an effective remedy, there would be a greater need for scrutiny by the Court and the individual would not need to demonstrate the existence of any risk that secret surveillance measures were applied to him. By contrast, if the national system provides for effective remedies, the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures only if he is able to show that, due to his personal situation, he is potentially at risk of being subjected to such measures (*Roman Zakharov*, cited above, § 171).

393. In the present case the Court has accepted that the IPT offers an effective remedy to anyone who wishes to complain about an interference with his or her communications by the United Kingdom authorities (see paragraphs 250-266 above).It has jurisdiction to investigate any complaint that a person's communications have been intercepted and, where interception has occurred, to examine the authority for such interception (see paragraph 124 above). This jurisdiction clearly extends to complaints about the receipt of intelligence from foreign intelligence services. Indeed, in the *Liberty* proceedings the IPT considered the applicants' complaints about both the section 8(4) regime and the intelligence sharing regime with equal diligence (see paragraphs 32-40 above). Consequently, the applicants can only claim to be "victims" on account of the mere existence of the intelligence sharing regime if they are able to show that, due to their personal situation, they were potentially at risk of having their communications obtained by the United Kingdom authorities through a

request to a foreign intelligence service (see *Roman Zakharov*, cited above, § 171).

394. According to Chapter 12 of the IC Code, absent exceptional circumstances intelligence can only be requested from third countries where there is already a section 8(1) or section 8(4) warrant in place. This means that there must either be an Article 8(1) warrant in relation to the subject at issue, or a section 8(4) warrant and accompanying certificate which covers the subject's communications (see paragraph 90 above). However, section 8(4) warrants are relatively broad in scope, and the Court has already considered the general terms in which both warrants and accompanying certificates are drafted (see paragraphs 156 and 341 above). Moreover, it is clear from the *Liberty* proceedings that at least two of the applicants in the third of the joined cases had their communications lawfully intercepted and selected for examination by the United Kingdom intelligence services under the section 8(4) regime (see paragraphs 54 and 55 above). While there is no reason to believe that these applicants were themselves of interest to the intelligence services, their communications could have been obtained lawfully under the section 8(4) regime if, as they claim, they were in contact with persons who were. Similarly, their communications could lawfully be requested from a third country under the intelligence sharing regime if they were in contact with an individual who was the subject of a request.

395. The Court would therefore accept, on the basis of the information submitted to it, that the applicants were potentially at risk of having their communications requested from a foreign intelligence service. In addition, it would accept that they were also potentially at risk of having their communications obtained by a foreign intelligence service. Although the United States of America is not the only country from which the authorities of the respondent State might request intelligence, the submissions before this Court – and before the IPT – focused on the receipt of information from the NSA. While PRISM is a targeted scheme which allows intelligence material to be obtained from Internet Service Providers ("ISPs"), Upstream appears to be a bulk interception scheme similar to the section 8(4) regime. In other words, it permits broad access to global data, in particular that of non-US citizens, which can then be collected, stored and searched using keywords.

396. In light of the foregoing considerations, the Court would accept that the applicants were potentially at risk of having their communications obtained by the intelligence services of the respondent State under the intelligence sharing regime. As such, it finds that they can claim to be victims, within the meaning of Article 34 of the Convention, of the violation alleged to flow from the intelligence sharing regime.

397. The Court notes that this complaint is not manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention. It further notes

that it is not inadmissible on any other grounds. It must therefore be declared admissible.

2. Merits

(a) The parties' submissions

(i) The applicants

398. The applicants submitted that even following the 9 October disclosure, there remained no basis in law for the intelligence sharing carried out by the intelligence services, and there was certainly no regime which satisfied the Court's "quality of law" requirements.

399. With regard to the test to be applied, the applicants contended that an interference with the rights protected by Article 8 of the Convention was no less serious when a third State shared the intelligence with the respondent State than when the respondent State conducted the surveillance itself. In *R.E.* the Court held that in determining whether the six minimum requirements applied the decisive factor would be the level of interference with an individual's right to respect for his or private life, and not the technical definition of that interference (*R.E.*, cited above, § 130). Since the degree of interference caused by the receipt of intelligence from third countries was similar to that caused by direct interception on the part of the respondent State, how that interference was technologically achieved should be irrelevant.

400. In the opinion of the applicants, the publication of the revised IC Code in 2016 was insufficient the remedy the flaws in the regime identified by the IPT as it simply applied the inadequate RIPA regime to the obtaining of data intercepted by a foreign Government.

(ii) The Government

401. The Government submitted that the intelligence sharing regime now had a basis in domestic law (namely, the Security Services Act 1989 ("the SSA") and the Intelligence Services Act 1994 ("the ISA"), as read with the Counter Terrorism Act 2008 ("the CTA"); the Human Rights Act 1998 ("the HRA"); the Data Protection Act 1998 ("the DPA"); the Official Secrets Act 1989 ("the OSA"); and Chapter 12 of the IC Code) and that law was clearly accessible.

402. They further argued that it was foreseeable as the law indicated the scope of any discretion and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference. They did not accept that the six criteria set down in *Weber and Saravia* (see paragraph 307 above) applied to an intelligence sharing regime in the same way as they applied to an interception regime. In this regard, the Court had expressly recognised that the strict standards developed in intercept cases

did not necessarily apply in other surveillance cases (for example, *Uzun*, cited above). While some of the material obtained from foreign governments might be the product of intercept, that would not necessarily be the case and the intelligence services might not even know whether communications provided to them by a foreign Government were the product of intercept.

403. Even if the six minimum requirements did apply, the Government argued that they were satisfied. First, the regime was sufficiently clear as regards the circumstances in which the intelligence services could in principle obtain information from other States; they could only obtain information so far as it was necessary for the proper discharge of their functions, being the interests of national security, the economic well-being of the United Kingdom, and the prevention and detection of serious crime.

404. Moreover, the circumstances in which the intelligence agencies could obtain information under the intelligence sharing regime were defined and circumscribed by the IC Code. In this regard, the effect of Chapter 12 of the Code was to confirm that, other than in exceptional circumstances, the intelligence services could only request "raw intercept" from a foreign government if it concerned targets who were already the subject of an interception warrant under Part I of RIPA, that material could not be obtained by the intelligence services themselves, and it was necessary and proportionate to obtain it. In the absence of a warrant, a request could only be made if it did not amount to a deliberate circumvention, or otherwise frustrate the objectives, of RIPA. Furthermore, any request made in the absence of a warrant would be decided on by the Secretary of State personally, and if the request was for "untargeted" material, communications obtained could not be examined according to any of the factors mentioned in section 16(2) of RIPA.

405. The Government further contended that the intelligence sharing regime was sufficiently clear as regards the subsequent handling, use and possible onward disclosure of material. Not only were the intelligence services bound by the general constraints of proportionality in the HRA and the fifth and seventh data protection principles, but Chapter 12 of the IC Code also provided that intercepted communications data or content received from another State, regardless of whether it was solicited or unsolicited, analysed or unanalysed, was subject to exactly the same rules and safeguards as material obtained directly by the intelligence services by interception under RIPA. In other words, the safeguards set out in section 15 of RIPA also applied to intercept material obtained under the intelligence sharing regime.

406. Finally, the Government pointed out that the intelligence sharing regime was subject to the same oversight mechanisms as the section 8(4) regime, and none of these oversight bodies had revealed any deliberate abuse by the intelligence services of their powers. Furthermore, no evidence

was found to suggest that the intelligence services had – or had attempted – to use the intelligence sharing regime to circumvent RIPA.

(b) The submissions of the third parties

(i) The Electronic Privacy Information Center ("EPIC")

407. EPIC submitted that the evolving technologies of the NSA and other intelligence agencies had created an almost unlimited ability to access, store and use personal information and private communications globally. However, no US law or regulation prohibited the NSA from conducting warrantless surveillance on foreign citizens abroad. Furthermore, in recent years the US had failed to adopt any meaningful reforms which would have provided adequate privacy and data protection safeguards for non-US persons.

(ii) Access Now

408. Access Now contended that while Mutual Legal Assistance Treaties ("MLATs") offered a transparent and formal process for one State party to request intelligence for another, the operation of secret signals intelligence programmes (for example, the Five Eyes intelligence sharing network of which the United Kingdom, the US, Australia, Canada and New Zealand were members) were not transparent and were prohibited by international human rights standards. Such secret programmes were not necessary, since the relevant intelligence could be obtained under MLATs.

(iii) Bureau Brandeis

409. The members of the Bureau Brandeis coalition were plaintiffs in a case against the Netherlands. The Dutch authorities had accepted that data was exchanged with foreign intelligence partners (including the US) and that it could not be excluded that they had received information acquired by foreign services using methods that might infringe human rights. The coalition brought proceedings in which they argued that the NSA's mass data collection programs violated human rights guaranteed by the Convention. However, the Hague District Court said that under Dutch law, Dutch intelligence services were allowed to collaborate with the NSA, and the NSA was in turn bound by US law which, in general, did not conflict with the Convention's privacy requirements. The court further held that because the raw data was shared in bulk, less stringent safeguards were necessary than would apply when the data was examined and used, as there was a difference between receiving data and using it for individual cases. An appeal against this decision was dismissed in March 2017.

410. In their third party intervention before this Court, the coalition argued that the sharing of intelligence should only be permitted if it was accompanied by sufficient safeguards and the foreign authority had a sound

legal basis for capturing the material. Otherwise, there could be a circumvention of the protection provided by Article 8 of the Convention. In other words, States should not be allowed to obtain material from foreign authorities that they could not lawfully capture themselves.

(iv) Center for Democracy and Technology ("CDT") and Pen American Center ("PEN America")

411. CDT and PEN America submitted that the interception regimes operated by the NSA would satisfy neither the "in accordance with the law" nor the "proportionality" requirements of Article 8 of the Convention, and these deficiencies tainted the lawfulness of the United Kingdom's intelligence sharing regime.

(v) The International Commission of Jurists ("ICJ")

412. The ICJ referred the Court to Articles 15 and 16 of the Articles of State Responsibility of the International Law Commission ("the ILC Articles"). They contended that, pursuant to Article 15, a Contracting State could be responsible for mass surveillance conducted by a non-Contracting State if they were acting in organised and structured forms of co-operation; and that, pursuant to Article 16, a Contracting State could be responsible for mass surveillance conducted by a non-Contracting State if it contributed to the surveillance programme and had actual or constructive knowledge of the breaches of international human rights obligations inherent in the system. The ICJ further submitted that Contracting States participating in or contributing to a mass surveillance programme were obliged to establish a system of safeguards for the protection of Article 8 rights, and were also under a duty to protect persons within their jurisdiction from violations of Article 8 rights caused by mass surveillance programmes.

(vi) Open Society Justice Initiative ("OSJI")

413. OSJI argued that States should not receive or request data from a third party in a manner that circumvents individuals' Article 8 rights. To ensure that this does not happen, they must put in place safeguards at the point when the material is first gathered, including prior scrutiny of the human rights record and interception laws and practices in the foreign State, and independent, preferably judicial, *a posteriori* oversight of any sharing arrangements to ensure that the safeguards are in place and enforced.

(vii) The Law Society of England and Wales

414. The Law Society previously submitted that the RIPA regime and associated Codes provided no robust or transparent safeguards for legally privileged material. Since the same safeguards applied to privileged material obtained by foreign States and disclosed to the intelligence services of the United Kingdom, the same deficiencies also tainted that regime.

(viii) Human Rights Watch ("HRW")

415. Although the present applications focused on the receipt of foreign intelligence from the United States, HRW believed that the network of States with which communications intelligence was shared was vastly larger. For example the "Five Eyes Alliance" comprised the United Kingdom, the United States, Australia, Canada and New Zealand, and there were also thought to be other, more restricted intelligence sharing coalitions (for example, the "Nine Eyes", adding Denmark, France, the Netherlands and Norway; the "Fourteen Eyes", adding Germany, Belgium, Italy, Spain and Sweden; and the "Forty-One Eyes", adding in others in the allied coalition in Afghanistan).

(c) The Court's assessment

(i) The scope of the applicants' complaints

416. This is the first time that the Court has been asked to consider the Convention compliance of an intelligence sharing regime. While the operation of such a scheme might raise a number of different issues under the Convention, in the present case the applicants' complaints focus on the Article 8 compliance of the regime by which the United Kingdom authorities request and receive intelligence from foreign Governments. The applicants do not complain about the transfer of intelligence from the United Kingdom intelligence services to foreign counterparts; nor do they invoke any other Convention Articles.

417. In the *Liberty* proceedings (in which the IPT was only concerned with the receipt of information from the United States) the applicants submitted that information acquired from the NSA fell into three categories: material which the NSA had provided to the United Kingdom intelligence services unsolicited, and which on its face derived from intercept; communications which the United Kingdom intelligence services had either asked the NSA to intercept, or to make available to them as intercept; and material obtained by the NSA other than by the interception of communications. Although the complaint before the Court is somewhat wider than the one which was before the IPT, the applicants in the first of the joined cases having complained about the receipt of information from any foreign Government, the categories identified by the IPT are nevertheless apposite. As the Government, at the hearing, informed the Court that it was "implausible and rare" for intercept material to be obtained "unsolicited", the Court will restrict its examination to material falling into the second and third categories.

418. Material falling within the second category can be divided into two sub-categories: communications which the respondent State has asked a foreign intelligence service to intercept; and communications already intercepted by a foreign intelligence service, which are conveyed to the

authorities of the respondent State upon their request. The Court will first deal with these two sub-categories together, before proceeding to consider the third category separately.

(ii) The nature of the interference

419. The Court has already found that the applicants can claim to be victims of the alleged violation of Article 8 of the Convention occasioned by the existence of an intelligence sharing regime. However, it is important to clarify at the outset the nature of the interference under consideration.

420. Although the impugned regime concerns intercepted communications, the interference under consideration in this case does not lie in the interception itself, which did not, in any event, occur within the United Kingdom's jurisdiction, and was not attributable to that State under international law. As the communications are being intercepted by foreign intelligence agencies, their interception could only engage the responsibility of the respondent State if it was exercising authority or control over those agencies (see, for example, *Jaloud v. the Netherlands* [GC], no. 47708/08, §§ 139 and 151 ECHR 2014 and *Al-Skeini and Others v. the United Kingdom* [GC], no. 55721/07, §§ 130-139, ECHR 2011). Even when the United Kingdom authorities request the interception of communications (rather than simply the conveyance of the product of intercept), the interception would appear to take place under the full control of the foreign intelligence agencies. Some of the third parties have invoked the ILC Articles, but these would only be relevant if the foreign intelligence agencies were placed at the disposal of the respondent State and were acting in exercise of elements of the governmental authority of the respondent State (Article 6); if the respondent State aided or assisted the foreign intelligence agencies in intercepting the communications where that amounted to an internationally wrongful act for the State responsible for the agencies, the United Kingdom was aware of the circumstances of the internationally wrongful act, and the act would have been internationally wrongful if committed by the United Kingdom (Article 16); or if the respondent State exercised direction or control over the foreign Government (Article 17). There is no suggestion that this is the case.

421. Consequently, the interference lies in the receipt of the intercepted material and its subsequent storage, examination and use by the intelligence services of the respondent State.

(iii) The applicable test

422. As with any regime which provides for the acquisition of surveillance material, the regime for the obtaining of such material from foreign Governments must be "in accordance with the law"; in other words, it must have some basis in domestic law, it must be accessible to the person concerned and it must be foreseeable as to its effects (see *Roman Zakharov*,

cited above, § 228). Furthermore, it must be proportionate to the legitimate aim pursued, and there must exist adequate and effective safeguards against abuse. In particular, the procedures for supervising the ordering and implementation of the measures in question must be such as to keep the "interference" to what is "necessary in a democratic society" (see *Roman Zakharov*, cited above, § 232).

423. The parties dispute whether the six minimum requirements commonly applied in cases concerning the interception of communications (namely, the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their communications intercepted; a limit on the duration of interception; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which intercepted data may or must be erased or destroyed – see paragraph 307 above) should apply in the present case. It is true that the interference in this case is not occasioned by the interception of communications by the respondent State. However, as the material obtained is nevertheless the product of intercept, those requirements which relate to its storage, examination, use, onward dissemination, erasure and destruction must be present. Indeed, as the Venice Commission noted, as States could use intelligence sharing to circumvent stronger domestic surveillance procedures and/or any legal limits which their agencies might be subject to as regards domestic intelligence operations, a suitable safeguard would be to provide that the bulk material transferred could only be searched if all the material requirements of a national search were fulfilled and this was duly authorised in the same way as a search of bulk material obtained by the signals intelligence agency using its own techniques (see paragraph 216 above).

424. Furthermore, while the first and second of the six requirements may not be of direct relevance where the respondent State is not carrying out the interception itself, the Court is nevertheless mindful of the fact that if Contracting States were to enjoy an unfettered discretion to request either the interception of communications or the conveyance of intercepted communications from non-Contracting States, they could easily circumvent their obligations under the Convention. Consequently, the circumstances in which intercept material can be requested from foreign intelligence services must also be set out in domestic law in order to avoid abuses of power. While the circumstances in which such a request can be made may not be identical to the circumstances in which the State may carry out interception itself (since, if a State's own intelligence services could lawfully intercept communications themselves, they would only request this material from foreign intelligence services if it is not technically feasible for them to do so), they must nevertheless be circumscribed sufficiently to prevent –

insofar as possible – States from using this power to circumvent either domestic law or their Convention obligations.

(iv) Application of the test to material falling into the second category

(α) Accessibility

425. The statutory framework which permits the United Kingdom intelligence services to request intercepted material from foreign intelligence agencies is not contained in RIPA. The British-US Communication Intelligence Agreement of 5 March 1946 specifically permits the exchange of material between the United States and the United Kingdom. More generally, the SSA (see paragraphs 98-99 above) and the ISA (see paragraphs 100-103 above) set out the function of the intelligence services and require that there be arrangements for ensuring that no information is obtained by them except so far as necessary for the proper discharge of their functions; and that no information is disclosed by them except so far as necessary for that purpose or for the purpose of any criminal proceedings.

426. Details of the internal arrangements referred to in the SSA and ISA were disclosed during the *Liberty* proceedings (the 9 October disclosure – see paragraphs 26-30 above) and those details have now been incorporated into the most recent IC Code (see paragraph 109 above).

427. Consequently, the Court considers that there is now a basis in law for the requesting of intelligence from foreign intelligence agencies, and that that law is sufficiently accessible. Furthermore, the regime clearly pursues several legitimate aims, including the interests of national security, public safety and the economic well-being of the country, the prevention of disorder or crime, and the protection of the rights and freedoms of others. It therefore falls to the Court to assess the foreseeability and necessity of the regime. As already indicated, it will do so by examining whether the law meets the following requirements by indicating: the circumstances in which intercept material can be requested; the procedure to be followed for examining, using and storing the material obtained; the precautions to be taken when communicating the material obtained to other parties; and the circumstances in which the material obtained must be erased or destroyed (see the third to sixth safeguards referred to in paragraph 307 above).

(β) The circumstances in which intercept material can be requested

428. Chapter 12 of the IC Code (see paragraph 109 above) states that, save in exceptional circumstances, the intelligence services may only make a request to a foreign government for unanalysed intercepted communications and/or associated communications data if an interception warrant under RIPA has already been issued by the Secretary of State, the assistance of the foreign government is necessary to obtain the particular

communications because they cannot be obtained under the existing warrant, and it is necessary and proportionate for the intercepting agency to obtain those communications. A RIPA interception warrant means either a section 8(1) warrant in relation to the subject at issue; a section 8(4) warrant and an accompanying certificate which includes one or more "descriptions of intercepted material" covering the subject's communications; or, where the subject is known to be within the British Islands, a section 8(4) warrant and an accompanying certificate which includes one or more "descriptions of intercepted material" covering his or her communications, together with an appropriate section 16(3) modification.

429. Where exceptional circumstances exist, a request for communications may be made in the absence of a relevant RIPA interception warrant only if it does not amount to a deliberate circumvention of RIPA or otherwise frustrate its objectives (for example, because it is not technically feasible to obtain the communications via RIPA interception), and it is necessary and proportionate for the intercepting agency to obtain those communications. In such a case the request must be considered and decided on by the Secretary of State personally, and, pursuant to the revised IC Code, notified to the Interception of Communications Commissioner (see paragraph 109 above). According to information disclosed during the *Liberty* proceedings, and confirmed in the Government's submissions in the present case, no request for intercept material has ever been made in the absence of an existing RIPA warrant.

430. In light of the above considerations, the Court considers that the circumstances in which the respondent State may request interception or the conveyance of intercepted material are sufficiently circumscribed in domestic law to prevent the State from using this power to circumvent either domestic law or its Convention obligations.

(γ) Procedure to be followed for storing, accessing, examining and using the material obtained

431. By virtue of section 19(2) of the Counter-Terrorism Act 2008 ("CTA" – see paragraph 103), information obtained by any of the intelligence services in connection with the exercise of any of their functions may be used in connection with the exercise of any of their other functions. However, the intelligence services are data controllers for the purposes of the Data Protection Act 1998 and are required to comply with the data protection principles in Part 1 of Schedule 1 to the DPA. While compliance with these principles is subject to exemption by ministerial certificate, they cannot be exempted from the obligation to comply with the fifth and seventh data protection principles, which provide that personal data processed for any purpose shall not be kept for longer than is necessary for that purpose; and appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data

and against accidental loss or destruction of, or damage to, personal data. A member of the intelligence services commits an offence under section 1(1) of the OSA (see paragraph 107 above) if he discloses, without lawful authority, any information relating to security or intelligence which is, or has been, in his possession by virtue of his position.

432. More specifically, Chapter 12 of the IC Code makes it clear that where intercepted communications content or communications data are obtained by the intelligence services from a foreign government in circumstances where the material identifies itself as the product of an interception, the communications content and communications data must be subject to the same internal rules and safeguards that apply to the same categories of content or data when they are obtained directly by the intelligence services as a result of interception under RIPA (see paragraph 109 above). This means that the safeguards in section 15 and 16 of RIPA, as supplemented by Chapter 7 of the IC Code, apply equally to intercepted communications and communications data obtained from foreign governments.

433. The Court has already given careful consideration to the safeguards in section 15 and 16 of RIPA, as supplemented by Chapter 7 of the IC Code, in its assessment of the section 8(4) regime (see paragraphs 361-363 above). In brief, material obtained from foreign intelligence agencies must be stored securely and must not be accessible to persons without the required level of security clearance. Access by the analyst is limited to a defined period of time, and if renewed, the record must be updated giving reasons for renewal. Before being able to examine material obtained from foreign intelligence agencies, specially authorised and vetted analysts must make a record of why access to the material is necessary for one of the statutory purposes set out in section 5(3) of RIPA, and proportionate. They cannot select material for examination using criteria that refer to the communications of individuals known currently to be in the British Islands (unless there is a warrant with a section 16(3) modification, or if, in the absence of a warrant, the Secretary of State has personally considered and approved the examination of those communications by reference to such factors).

434. Although the IPT had, in the *Liberty* proceedings, expressed concern that the section 16(2)(a) and (b) safeguards (which prevent intercepted material being selected for examination by reference to an individual known to be in the British Islands) did not appear to apply to material obtained from foreign governments in the absence of a warrant, the IC Code has since been amended to address this concern. Paragraph 12.5 now expressly provides that if a request made in the absence of a warrant is approved by the Secretary of State other than in relation to specific selectors, any communications obtained must not be examined by the intelligence services according to any factors as are mentioned in

section 16(2)(a) and (b) of RIPA unless the Secretary of State has personally considered and approved the examination of those communications by reference to such factors (see paragraph 110 above).

435. In light of the foregoing, the Court would accept that the provisions relating to the storing, accessing, examining and using such material are sufficiently clear.

(δ) Procedure to be followed for communicating the material obtained to other parties

436. As with material intercepted directly pursuant to a RIPA warrant (see paragraphs 365-367 above), disclosure of material obtained from foreign intelligence agencies must be limited to the minimum necessary for the "authorised purposes" mentioned in section 5(3) of RIPA. In addition, disclosure to persons who have not been appropriately vetted is prohibited and material may only be disclosed to a person whose duties, which must relate to one of the authorised purposes, are such that he or she needs to know about the material to carry out those duties. In the same way, only so much of the intercepted material may be disclosed as the recipient needs.

437. Section 19(3), (4) and (5) of the CTA further provide that information obtained by MI5 and MI6 for the purposes of any of their functions may be disclosed by them for the purpose of the proper discharge of their functions; in the interests of national security; for the purpose of the prevention or detection of serious crime; or for the purpose of any criminal proceedings. Information obtained by GCHQ may be disclosed by it for the purpose of the proper discharge of its functions or for the purpose of any criminal proceedings (see paragraphs 104-105 above).

438. Moreover, a member of the intelligence services commits an offence under section 1(1) of the OSA if without lawful authority he discloses any information, document or other article relating to security or intelligence which is, or has been, in his possession by virtue of his position as a member of any of those services (see paragraph 107 above).

439. In light of the foregoing, the Court would also accept that the provisions relating to the procedure to be followed for communicating the material obtained to other parties are sufficiently clear.

(ε) The circumstances in which the material obtained must be erased or destroyed

440. Section 15(3) of RIPA and paragraph 7.8 of the IC Code require that every copy (together with any extracts and summaries) be destroyed securely as soon as retention is no longer necessary for any of the section 5(3) purposes (see paragraphs 74 and 90 above).

(ζ) Supervision and remedies

441. In nearly every case either a section 8(1) or 8(4) warrant will be in place, meaning that the Secretary of State (and, following the coming into force of IPA 2016, a judicial commissioner) will have authorised the interception. In exceptional circumstances, when a warrant is not in place, the Secretary of State must personally consider and decide upon the request, and the Interception of Communications Commissioner (now the Investigatory Powers Commissioner) must be notified. Therefore, in every case where a request has been made the Secretary of State will have deemed the interception to be necessary and proportionate (in the Convention sense).

442. Further oversight of the intelligence sharing regime is provided by the ISC, a cross-party Committee of Members of Parliament which exercises wide powers. Following an extensive review, on 13 July 2013 the ISC published a report in which it concluded that allegations "that GCHQ circumvented UK law by using the NSA's PRISM programme to access the content of private communications" were unfounded as GCHQ had complied with its statutory duties contained in the ISA (see paragraphs 148-150 above).

443. Additional oversight was afforded by the Interception of Communications Commissioner, who was independent from both Government and the intelligence services. He was under a duty by section 58(4) of RIPA to make an annual report to the Prime Minister regarding the carrying out of his functions, which had to be laid before Parliament. As already noted, the Interception of Communications Commissioner has now been replaced by the Investigatory Powers Commissioner. On 17 October 2017, in a reply to a question posed by, *inter alia*, Privacy International, the new Commissioner confirmed that, like his predecessor, he had the power to oversee the Government's intelligence sharing agreements, and that he intended to use those powers actively to ensure effective oversight.

444. A final level of oversight is provided by the IPT, and its effectiveness was demonstrated in the *Liberty* proceedings by the fact that it was able to ensure disclosure of certain arrangements which have now been incorporated into the IC Code (see paragraph 109 above).

(η) Proportionality

445. The Court has always been acutely conscious of the difficulties faced by States in protecting their populations from terrorist violence, which constitutes, in itself, a grave threat to human rights (see, for example, *Lawless v. Ireland (no. 3)*, 1 July 1961, §§ 28–30, Series A no. 3; *Ireland v. the United Kingdom*, 18 January 1978, Series A no. 25; and *Öcalan v. Turkey* [GC], no. 46221/99, § 179, ECHR 2005-IV) and in recent years it has expressly acknowledged – in response to complaints invoking a wide

range of Convention Articles – the very real threat that Contracting States currently face on account of international terrorism (see, for example, *Chahal v. the United Kingdom*, 15 November 1996, § 79, *Reports of Judgments and Decisions* 1996-V; *A. and Others v. the United Kingdom* [GC], no. 3455/05, § 181, ECHR 2009; *A. v. the Netherlands*, no. 4900/06, § 143, 20 July 2010; *Trabelsi v. Belgium*, no. 140/10, § 117, ECHR 2014 (extracts); and *Othman (Abu Qatada) v. United Kingdom*, no. 8139/09, § 183, ECHR 2012).

446. Faced with such a threat, the Court has considered it legitimate for Contracting States to take a firm stand against those who contribute to terrorist acts (see *Othman*, cited above, § 183). Due to the nature of global terrorism, and in particular the complexity of global terror networks, the Court accepts that taking such a stand – and thus preventing the perpetration of violent acts endangering the lives of innocent people – requires a flow of information between the security services of many countries in all parts of the world. As, in the present case, this "information flow" was embedded into a legislative context providing considerable safeguards against abuse, the Court would accept that the resulting interference was kept to that which was "necessary in a democratic society".

(θ) Conclusions

447. In light of the foregoing considerations, the Court considers that the domestic law, together with the clarifications brought by the amendment of the IC Code, indicate with sufficient clarity the procedure for requesting either interception or the conveyance of intercept material from foreign intelligence agencies. In this regard, it observes that the high threshold recommended by the Venice Commission – namely, that the material transferred should only be able to be searched if all the material requirements of a national search were fulfilled and this was duly authorised in the same way as a search of bulk material obtained by the signals intelligence agency using its own techniques – is met by the respondent State's regime. The Court further observes that there is no evidence of any significant shortcomings in the application and operation of the regime. On the contrary, following an investigation the ISC found no evidence whatsoever of abuse.

448. There has accordingly been no violation of Article 8 of the Convention.

(v) Application of the test to material falling into the third category

449. The third category of material identified at paragraph 417 above is material obtained by foreign intelligence agencies other than by the interception of communications. However, as the applicants have not specified the kind of material foreign intelligence agencies might obtain by methods other than interception they have not demonstrated that its

acquisition would interfere with their Article 8 rights. As such, the Court considers that there is no basis upon which it could find a violation of Article 8 of the Convention.

C. The Chapter II regime

450. The applicants in the second of the joined cases complained that the regime for the acquisition of communications data under Chapter II of RIPA was incompatible with their rights under Article 8 of the Convention.

1. Admissibility

451. In both their application to the Court and their initial observations, the applicants in the second of the joined cases incorrectly referred to the Chapter II regime as a regime for the interception of communications data. The Court observes, however, that it is not an interception regime, but rather permits certain public authorities to acquire communications data from Communications Service Providers ("CSPs"). In view of the "fundamental legal misunderstanding" upon which the complaint was originally founded, the Government submitted that the applicants have put forward no factual basis whatsoever for concluding that their communications were acquired in this way, and that they did not contend that they had been affected, either directly or indirectly, by the regime. The Government further argued that neither of the two conditions identified by the Court in *Roman Zakharov* (cited above, § 171) were satisfied in respect of the Chapter II regime: the applicants did not belong to a group "targeted" by the contested legislation, and they had available to them an effective domestic remedy. Consequently, they could not claim to be victims of the alleged violation within the meaning of Article 34 of the Convention.

452. The applicants, on the other hand, submitted that they were entitled to bring the present complaint since they could possibly have been affected by the impugned legislation and no effective remedy was available at the domestic level.

453. In assessing victim status the Court is predominantly concerned with whether an effective remedy existed which permitted a person who suspected that he or she was subject to secret surveillance to challenge that surveillance (see *Roman Zakharov*, cited above, § 171). In the present case, although the Court accepted that there existed special circumstances absolving the applicants from the requirement that they first bring their complaints to the IPT (see paragraph 268 above), it nevertheless found that the IPT was an effective remedy, available in theory and practice, which was capable of offering redress to applicants complaining of both specific incidences of surveillance and the general Convention compliance of surveillance regimes (see paragraphs 250-266 above). Consequently, the applicants can only claim to be "victims" on account of the mere existence

of the Chapter II regime if they are able to show that, due to their personal situation, they were potentially at risk of having their communications data obtained by the United Kingdom authorities through a request to a CSP (see *Roman Zakharov*, cited above, § 171).

454. In this regard, the Court notes that the Chapter II regime is not a regime for the bulk acquisition of communications data; rather, as stated previously, it permits public authorities to request specific communications data. Nevertheless, a large number of public authorities are entitled to make such requests, and the grounds on which a request might be made are relatively wide. Given that the applicants in the second of the joined cases are investigative journalists who have reported on issues such as CIA torture, counterterrorism, drone warfare, and the Iraq war logs, the Court would accept that they were potentially at risk of having their communications obtained by the United Kingdom authorities either directly, through a request to a CSP for their communications data, or indirectly, through a request to a CSP for the communications data of a person or organisation they had been in contact with.

455. The Court would therefore accept that they were "victims" within the meaning of Article 34 of the Convention. As this complaint is not inadmissible on any other grounds, it must be declared admissible.

2. Merits

(a) The parties' submissions

(i) The applicants

456. The applicants submitted that Chapter II of RIPA permitted the obtaining of communications data in a wide range of ill-defined circumstances, without proper safeguards. In particular, they submitted that the legal framework and attendant safeguards were informed by a fundamental but erroneous premise; namely, that the obtaining of communications data was necessarily less intrusive than the interception of content. In particular, the applicants complained that in most cases authorisation for the acquisition of communications data was provided by a designated person, who was not sufficiently independent of the executive or even of the agency requesting the disclosure.

457. Furthermore, they complained that Chapter II provided few limitations as to the basis on which communications data could be acquired, since section 22 of RIPA allowed a designated person to authorise the acquisition of communications data on a broad range of grounds, provided that he or she believed it "necessary". Finally, they argued that there were very few safeguards in respect of the handling and exploitation of communications data.

(ii) The Government

458. The Government pointed out that as the Chapter II regime was a targeted regime, there was nothing "unintentional" about its operation. On the contrary, the acquisition of communications data under it would always be intentional. It was therefore to be distinguished from regimes for the bulk interception or bulk acquisition of data.

459. The Government further argued that the amended Acquisition and Disclosure of Communications Data Code of Practice ("the ACD Code") provided adequate safeguards in respect of the retention of communications data acquired under the Chapter II regime, and that the Interception of Communications Commissioner provided an important degree of oversight of the operation of the regime.

(b) The Court's assessment

(i) Existing case-law on the acquisition of communications data

460. To date, the Court has only twice been called on to consider the Convention compliance of a regime for the acquisition by a public authority of communications data from a CSP: in *Malone* and, more recently, in *Ben Faiza* (both cited above). In *Malone*, the authorities had obtained the numbers dialled on a particular telephone and the time and duration of the calls from the Post Office, which, as the supplier of the telephone service, had acquired this data legitimately by a process known as "metering". While the Court accepted that the use of the data could give rise to an issue under Article 8 of the Convention, it considered that "by its nature" it had to be distinguished from the interception of communications, which was "undesirable and illegitimate in a democratic society unless justified" (see *Malone*, cited above, § 84). However, it was not necessary for the Court to consider this issue in any further detail, since, in the absence of any legal framework governing the acquisition of records from the Post Office, the Court found that the interference had no basis in domestic law (see *Malone*, cited above, § 87).

461. While *Malone* is now thirty-four years old, the *Ben Faiza* judgment was delivered in February 2018. In that case the Court was considering an order issued to a mobile telephone operator to provide lists of incoming and outgoing calls on four mobile telephones, together with the list of cell towers "pinged" by those telephones. Pursuant to the domestic law in question (Article 77-1-1 of the Criminal Procedure Code), prosecutors or investigators could, on the authorisation of the former, require establishments, organisations, persons, institutions and administrations to provide them with documents in their possession which were required for the purposes of the investigation. The Court accepted that the measure was "in accordance with the law", and that the law provided adequate safeguards against arbitrariness. In respect of those safeguards, the Court observed that

a request under Article 77-1-1 was subject to the prior authorisation of the public prosecutor's office; this obligation could not be derogated from under penalty of nullity of the act; and the legality of such a measure could be reviewed in subsequent criminal proceedings against the person concerned and, if found to be unlawful, the criminal courts could exclude the evidence so obtained (*Ben Faiza*, cited above, §§ 72-73).

462. In adopting this approach, the Court distinguished between methods of investigation which made it possible to identify the past geographical position of a person and those which made it possible to geolocate him or her in real time, indicating that the latter was more likely to violate the right to respect for private life. Consequently, in the view of the Court, the transmission to a judicial authority of existing data held by a public or private body was to be distinguished from the establishment of a surveillance system, such as the ongoing monitoring of a telephone line or the placing of a tracking device on a vehicle (*Ben Faiza*, cited above, § 74; see also paragraph 350 above).

463. The Court of Justice of the European Union has also addressed this issue. In *Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources and Others and Settinger and Others* (Cases C-293/12 and C-594/12), the CJEU considered the validity of the Data Retention Directive, and in *Secretary of State for the Home Department v. Watson and Others* (C-698/15), the validity of domestic legislation containing the same provisions as that directive (see paragraphs 224-234 above). While its focus was on the retention of data by CSPs, it also considered the question of access to retained data by the national authorities. In doing so, it indicated that access should be limited to what was strictly necessary for the objective pursued and, where that objective was fighting crime, it should be restricted to fighting serious crime. It further suggested that access should be subject to prior review by a court or independent administrative authority, and that there should be a requirement that the data concerned be retained within the European Union. In light of the CJEU's findings, Liberty sought to challenge Part 4 of the IPA, which included a power to issue "retention notices" to telecommunications operators requiring the retention of data. In response, the Government conceded that Part 4 was incompatible with fundamental rights in EU law since access to retained data was not limited to the purpose of combating "serious crime"; and access to retained data was not subject to prior review by a court or an independent administrative body. The High Court held that the legislation had to be amended by 1 November 2018 (see paragraph 196 above).

(ii) The approach to be taken in the present case

464. The appropriate test in the present case will therefore be whether the Chapter II regime was in accordance with the law; whether it pursued a legitimate aim; and whether it was necessary in a democratic society, having

particular regard to the question of whether it provided adequate safeguards against arbitrariness.

(iii) Examination of the Chapter II regime

465. No interference can be considered to be "in accordance with law" unless the decision occasioning it complies with the relevant domestic law. It is in the first place for the national authorities, notably the courts, to interpret and apply the domestic law: the national authorities are, in the nature of things, particularly qualified to settle issues arising in this connection. The Court cannot question the national courts' interpretation, except in the event of flagrant non-observance or arbitrariness in the application of the domestic legislation in question (see *Mustafa Sezgin Tanrıkulu*, cited above, § 53; see also, *mutatis mutandis*, *Weber and Saravia*, cited above, § 90).

466. The Court observes that the Chapter II regime has a clear basis in both section 22 of RIPA and the ACD Code. However, as a Member State of the European Union, the Community legal order is integrated into that of the United Kingdom and, where there is a conflict between domestic and law and EU law, the latter has primacy. Consequently, the Government have conceded that Part 4 of the IPA is incompatible with EU law because access to retained data was not limited to the purpose of combating "serious crime"; and access to retained data was not subject to prior review by a court or an independent administrative body. Following this concession, the High Court ordered that the relevant provisions of the IPA should be amended by 1 November 2018 (see paragraph 196 above).

467. It is therefore clear that domestic law, as interpreted by the domestic authorities in light of the recent judgments of the CJEU, requires that any regime permitting the authorities to access data retained by CSPs limits access to the purpose of combating "serious crime", and that access be subject to prior review by a court or independent administrative body. As the Chapter II regime permits access to retained data for the purpose of combating crime (rather than "serious crime") and, save for where access is sought for the purpose of determining a journalist's source, it is not subject to prior review by a court or independent administrative body, it cannot be in accordance with the law within the meaning of Article 8 of the Convention.

468. Accordingly, the Court finds that there has been a violation of Article 8 of the Convention.

III. ALLEGED VIOLATION OF ARTICLE 10 OF THE CONVENTION

469. The applicants in the third of the joined cases complained under Article 10 of the Convention about the section 8(4) regime and the intelligence sharing regime, arguing, in particular, that the protection

afforded by Article 10 was of critical importance to them as NGOs involved in matters of public interest, who were exercising a role of public watchdog of similar importance to that of the press; and the applicants in the second of the joined cases, being a journalist and newsgathering organisation, complained under Article 10 of the Convention about both the section 8(4) regime and the Chapter II regime.

470. Article 10 of the Convention provides as follows:

> "1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
>
> 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

A. Admissibility

1. The applicants in the third of the joined cases

471. The Court has already found that as a general rule the IPT has shown itself to be a remedy, available in theory and practice, which is capable of offering redress to applicants complaining about both specific incidences of surveillance and the general Convention compliance of a surveillance regime (see paragraphs 250-266 above). The Court has, however, accepted that there existed special circumstances absolving the applicants in the first and second of the joined cases from the requirement that they exhaust this remedy (see paragraph 268 above), but as the applicants in the third of the joined cases challenged the Convention compliance of both the section 8(4) regime and the intelligence sharing regime before the IPT, they cannot benefit from the "absolution" afforded to the other applicants. Therefore, as they did not complain before the IPT that the intelligence sharing regime was incompatible with Article 10 of the Convention, this complaint must be declared inadmissible for failure to domestic remedies within the meaning of Article 35 § 1 of the Convention.

472. Furthermore, although these applicants did complain before the IPT that the section 8(4) regime was not compatible with Article 10, in doing so they primarily relied on the same arguments invoked in respect of their Article 8 complaint. Insofar as they sought to argue that Article 10 could apply to their investigatory activities as NGOs, this argument was only raised on 17 November 2014 (the first and second open hearings having taken place in July and October 2014). As the IPT considered that this

argument could have been raised at any time, in its judgment it had been raised far too late to be incorporated into the ambit of the *Liberty* proceedings (see paragraph 47 above).

473. Therefore, with regard to the Article 8(4) complaint, the Court finds that insofar as the applicants in the third of the joined cases seek to rely on the special protection afforded by Article 10 of the Convention to journalists, they have not exhausted domestic remedies within the meaning of Article 35 § 1 of the Convention. Their complaints under this head must also be declared inadmissible.

474. Finally, the Court considers that the more general Article 10 complaint – which the applicants raised before the IPT in good time – gives rise to no separate argument over and above that arising out of Article 8 of the Convention. It is not, therefore, necessary to examine this complaint.

2. The applicants in the second of the joined cases

475. As the Court has acknowledged that the applicants in the second of the joined cases were, exceptionally, absolved from the requirement that they first bring their complaints to the IPT, they cannot be said to have failed to exhaust domestic remedies within the meaning of Article 35 § 1 of the Convention. As their complaints are not inadmissible on any other ground, they must, therefore, be declared admissible.

476. Moreover, the applicants in the second of the joined cases are a journalist and a newsgathering organisation, who complain about the interference with confidential journalistic material occasioned by the operation of both the section 8(4) regime and the Chapter II regime. As such, their complaints raise separate issues to those raised under Article 8 of the Convention, which will be examined below.

B. Merits

1. The parties' submissions

(a) The applicants

477. The applicants argued that as freedom of the press constituted one of the essential foundations of a democratic society, and the protection of journalistic sources was one of the cornerstones of freedom of the press, Article 10 of the Convention imposed additional and more exacting requirements where an interference gave rise to a significant risk of revealing journalistic sources or confidential journalistic material. In this regard, they submitted that surveillance measures which ran a significant risk of identifying journalistic source material had to be justified by an "overriding public interest" (*Sanoma Uitgevers B.V.*, cited above, §§ 51 and 90, 14 September 2010 and *Goodwin v. the United Kingdom*, 27 March

1996, § 39 *Reports of Judgments and Decisions* 1996-II); and authorisation could only be granted by a judge or other independent adjudicative body.

478. The applicants submitted that as journalists involved in matters of public interest, who were exercising a role of public watchdog, the protection afforded by Article 10 was of critical importance to them.

479. In respect of the section 8(4) regime, the applicants argued that the interception of material gathered through bulk surveillance was not attended by adequate safeguards. First of all, the definition of "confidential journalistic material" in the IC Code of Practice was too narrow, as it was limited to material acquired for the purpose of journalism and held subject to an undertaking to hold it in confidence. This definition was inconsistent with the Court's broader definition (for example, in *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, no. 39315/06, § 86, 22 November 2012). Secondly, the regime did not comply with the strict requirements of Article 10 where surveillance measures might reveal journalistic source material (in the applicants' submissions, the existence of an "overriding public interest" and judicial – or at least independent – authorisation).

480. With regard to the Chapter II regime, the applicants complained that the ACD Code failed to recognise that communications data could be privileged, and that the obtaining of communications data which constituted confidential journalistic material was as intrusive as obtaining content, since a single piece of communications data could reveal the identity of a journalist's source, and when aggregated and subjected to modern data-mining technology, it could reveal an enormous range of (journalistically privileged) information. The applicants further complained that in most cases authorisation for the acquisition of communications data was provided by a designated person, who was not sufficiently independent of the executive, or even of the agency requesting the disclosure. While an additional safeguard now existed requiring that applications made in order to identify a journalist's source be authorised by a judge, they did not apply where the identification of the source was incidental rather than intended.

(b) The Government

481. In the Government's submissions, prior authorisation was the only respect in which the applicants contended that the position regarding the "in accordance with the law" test might differ under Article 10 from that under Article 8, and in respect of which they asserted that their identity as journalists might be material to the analysis. However, there was no authority in the Court's case-law for the proposition that prior judicial (or independent) authorisation was required for a strategic monitoring regime by virtue of the fact that some journalistic material might be intercepted in the course of that regime's operation. On the contrary, the Court had drawn a sharp and important distinction between the strategic monitoring of

communications and/or communications data, which might inadvertently "sweep up" some journalistic material, and measures that targeted journalistic material, particularly for the purposes of identifying sources, where prior authorisation would be required.

482. With regard to Chapter II of RIPA, the Government pointed out that pursuant to the amended Acquisition and Disclosure of Communications Data Code of Practice ("the ACD Code"), where the identification of a journalist's source was intended, judicial authorisation was required. As there was nothing "unintentional" about the operation of the Chapter II regime, the acquisition of communications data under it would always be intentional and further safeguards were not required for the unintentional acquisition of material disclosing a journalist's source.

483. The Government further argued that the ACD Code provided for the protection of confidential material, including journalistic material. Such material should only be retained where necessary and proportionate for one of the authorised purposes in section 15(4) of RIPA; it must be destroyed securely when its retention was no longer needed for those purposes; and, if retained, there had to be adequate information management systems in place to ensure that retention remained necessary and proportionate. Where it was retained or disseminated to an outside body, reasonable steps had to be taken to mark it as confidential, and where any doubt existed, legal advice had to be sought about its dissemination. Finally, any case where confidential material was retained had to be notified to the Commissioner as soon as reasonably practical and the material had to be made available to the Commissioner on request.

2. The submissions of the third parties

(a) The Helsinki Foundation for Human Rights

484. The Helsinki Foundation submitted that the protection of journalistic sources was undermined not only by the surveillance of the content of journalists' communications, but also by the surveillance of related metadata which could, by itself, allow for the identification of sources and informants. It was especially problematic that confidential information could be acquired without the journalists' knowledge or control, thereby depriving them of their right to invoke confidentiality, and the ability of their sources to rely on guarantees of confidentiality.

(b) The National Union of Journalists ("NUJ") and the International Federation of Journalists ("IFJ")

485. The NUJ and the IFJ submitted that the confidentiality of sources was indispensable for press freedom. They also expressed concern about the possible sharing of data retained by the United Kingdom with other countries. If confidential journalistic material were to be shared with a

country which could not be trusted to handle it securely, it could end up in the hands of people who would harm the journalist or his or her source. In the interveners' view, the safeguards in the updated IC and ACD Codes of Practice were not adequate, especially where the journalist or the identification of his or her source was not the target of the surveillance measure.

(c) The Media Lawyers' Association ("MLA")

486. The MLA expressed deep concern that domestic law was moving away from the strong presumption that journalistic sources would be afforded special legal protection, since surveillance regimes allowed the authorities to intercept journalists' communications without the need for prior judicial authorisation. Since the protection of journalists' sources was one of the core components of Article 10, more robust protection was required.

3. The Court's assessment

(a) General principles

487. The Court reiterates that freedom of expression constitutes one of the essential foundations of a democratic society and that the safeguards to be afforded to the press are of particular importance. The protection of journalistic sources is one of the cornerstones of freedom of the press. Without such protection, sources may be deterred from assisting the press in informing the public about matters of public interest. As a result the vital public-watchdog role of the press may be undermined, and the ability of the press to provide accurate and reliable information may be adversely affected (see, *inter alia*, *Sanoma Uitgevers B.V.*, cited above, § 50; *Weber and Saravia*, cited above, § 143; *Goodwin*, cited above, § 39; and *Roemen and Schmit v. Luxembourg*, no. 51772/99, § 46, ECHR 2003-IV).

488. The Court has always subjected the safeguards for respect of freedom of expression in cases under Article 10 of the Convention to special scrutiny. Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society, an interference cannot be compatible with Article 10 of the Convention unless it is justified by an overriding requirement in the public interest (*Sanoma Uitgevers B.V.*, cited above, § 51; *Goodwin*, cited above, § 39; *Roemen and Schmit*, cited above, § 46; and *Voskuil v. the Netherlands*, no. 64752/01, § 65, 22 November 2007).

489. The Court has recognised that there is "a fundamental difference" between the authorities ordering a journalist to reveal the identity of his or her sources, and the authorities carrying out searches at a journalist's home and workplace with a view to uncovering his or her sources (compare *Goodwin*, cited above, with *Roemen and Schmit*, cited above, § 57). The

Court considered that the latter, even if unproductive, constituted a more drastic measure than an order to divulge the source's identity, since investigators who raid a journalist's workplace have access to all the documentation held by the journalist (*Roemen and Schmit*, cited above, § 57). However, the Court has also drawn a distinction between searches carried out on journalists' homes and workplaces "with a view to uncovering their sources", and searches carried out for other reasons, such as the obtaining of evidence of an offence committed by a person other than in his or her capacity as a journalist (*Roemen and Schmit*, cited above, § 52). Similarly, in *Weber and Saravia*, the only case in which the Court has considered, *in abstracto*, the Article 10 compliance of a secret surveillance regime on account of the potential for interference with confidential journalistic material, it considered it decisive that the surveillance measures were not aimed at monitoring journalists or uncovering journalistic sources. As such, it found that the interference with freedom of expression could not be characterised as particularly serious (*Weber and Saravia*, cited above, § 151).

(b) The application of the general principles to the present case

(i) The section 8(4) regime

490. With regard to the question of victim status, the Court recalls that in *Weber and Saravia* it expressly recognised that the impugned surveillance regime had interfered with the first applicant's freedom of expression as a journalist (*Weber and Saravia*, cited above, §§ 143-145). In the present case, the applicants in the second of the joined cases are journalists and can similarly claim to be "victims" of an interference with their Article 10 rights by virtue of the operation of the section 8(4) regime.

491. For the reasons set out in respect of the Article 8 complaint, the Court considers that – save for its concerns about the oversight of the selection process and the safeguards applicable to the selection of related communications data (see paragraph 387 above) – the section 8(4) regime was in accordance with the law (see paragraphs 387-388 above). Furthermore, it pursued the legitimate aims of protecting interests of national security, territorial integrity and public safety, and preventing disorder and crime.

492. With regard to "necessity", the Court reiterates that, having regard to the importance of the protection of journalistic sources for the freedom of the press in a democratic society, an interference could not be compatible with Article 10 of the Convention unless it was justified by an overriding requirement in the public interest (*Weber and Saravia*, cited above, § 149). In this regard, it notes that the surveillance measures under the section 8(4) regime – like those under the G10 Act which were considered in *Weber and Saravia* – are not aimed at monitoring journalists or uncovering journalistic

sources. Generally the authorities would only know when examining the intercepted communications if a journalist's communications had been intercepted. Consequently, it confirms that the interception of such communications could not, by itself, be characterised as a particularly serious interference with freedom of expression (*Weber and Saravia*, cited above, § 151). However, the interference will be greater should these communications be selected for examination and, in the Court's view, will only be "justified by an overriding requirement in the public interest" if accompanied by sufficient safeguards relating both to the circumstances in which they may be selected intentionally for examination, and to the protection of confidentiality where they have been selected, either intentionally or otherwise, for examination.

493. In this regard, paragraphs 4.1 – 4.8 of the IC Code require special consideration to be given to the interception of communications that involve confidential journalistic material and confidential personal information (see paragraph 90 above). However, these provisions appear to relate solely to the decision to issue an interception warrant. Therefore, while they might provide adequate safeguards in respect of a targeted warrant under section 8(1) of RIPA, they do not appear to have any meaning in relation to a bulk interception regime. Furthermore, the Court has already criticised the lack of transparency and oversight of the criteria for searching and selecting communications for examination (see paragraphs 339, 340, 345 and 387 above). In the Article 10 context, it is of particular concern that there are no requirements – at least, no "above the waterline" requirements – either circumscribing the intelligence services' power to search for confidential journalistic or other material (for example, by using a journalist's email address as a selector), or requiring analysts, in selecting material for examination, to give any particular consideration to whether such material is or may be involved. Consequently, it would appear that analysts could search and examine without restriction both the content and the related communications data of these intercepted communications.

494. Safeguards do exist in respect of the storing of confidential material once identified. For example, paragraph 4.29 of the IC Code (see paragraph 90 above) provides that such material should only be retained where it is necessary and proportionate for one of the authorised purposes in section 15(4) of RIPA, and it must be destroyed securely when it is no longer needed for one of these purposes. Furthermore, according to paragraph 4.30, if it is retained or disseminated to an outside body, reasonable steps should be taken to mark the information as confidential; and paragraph 4.31 requires that the Interception of Communications Commissioner be notified of the retention of such material as soon as reasonably practicable, and such material should be made available to him on request.

495. Nevertheless, in view of the potential chilling effect that any perceived interference with the confidentiality of their communications and, in particular, their sources might have on the freedom of the press and, in the absence of any "above the waterline" arrangements limiting the intelligence services' ability to search and examine such material other than where "it is justified by an overriding requirement in the public interest", the Court finds that there has also been a violation of Article 10 of the Convention.

(ii) The Chapter II regime

496. The applicants in the second of the joined cases also complained under Article 10 of the Convention about the regime for the acquisition of communications data from CSPs.

497. In considering the applicants' Article 8 complaint, the Court concluded that the Chapter II regime was not in accordance with the law as it permitted access to retained data for the purpose of combating crime (rather than "serious crime") and, save for where access was sought for the purpose of determining a journalist's source, it was not subject to prior review by a court or independent administrative body (see paragraph 467 above).

498. The Court acknowledges that the Chapter II regime affords enhanced protection where data is sought for the purpose of identifying a journalist's source, In particular, paragraph 3.77 of the ACD Code provides that where an application is intended to determine the source of journalistic information, there must be an overriding requirement in the public interest, and such applications must use the procedures of the Police and Criminal Evidence Act 1984 ("PACE") to apply to a court for a production order to obtain this data (see paragraph 117 above). Pursuant to Schedule 1 to PACE, an application for a production order is made to a judge and, where the application relates to material that consists of or includes journalistic material, the application should be made *inter partes* (see paragraph 121 above). The internal authorisation process may only be used if there is believed to be an immediate threat of loss of human life, and that person's life might be endangered by the delay inherent in the process of judicial authorisation (paragraphs 3.76 and 3.78-3.84 of the ACD Code – see paragraph 117 above).

499. Nevertheless, these provisions only apply where the purpose of the application is to determine a source; they do not, therefore, apply in every case where there is a request for the communications data of a journalist, or where such collateral intrusion is likely. Furthermore, in cases concerning access to a journalist's communications data there are no special provisions restricting access to the purpose of combating "serious crime". Consequently, the Court considers that the regime cannot be "in accordance with the law" for the purpose of the Article 10 complaint.

(iii) Overall conclusion

500. In respect of the complaints under Article 10 of the Convention, the Court therefore finds a violation in respect of the section 8(4) regime and the Chapter II regime.

IV. ALLEGED VIOLATION OF ARTICLE 6 OF THE CONVENTION

501. The applicants in the third of the joined cases further complained under Article 6 of the Convention that the limitations inherent in the IPT proceedings were disproportionate and impaired the very essence of their right to a fair trial.

502. Article 6 provides, as relevant:

> "1. In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice."

503. In particular, the applicants contended that there was a lack of independence and impartiality on the part of the IPT, evidenced by the fact that in November 2007 there had been a secret meeting between it and the Security Services which, they alleged, resulted in the adoption of a protocol pursuant to which MI5 agreed not to search or disclose any bulk data holdings relating to complainants; that they were not effectively represented in the closed proceedings; that the IPT failed to require the defendants to disclose key internal guidance; and that, following the hearing, the IPT had made its determination in favour of the wrong party.

504. The Government submitted that Article 6 of the Convention did not apply to surveillance proceedings, since the Commission and the Court had consistently held that decisions authorising surveillance did not involve the determination of "civil rights and obligations" within the meaning of Article 6 § 1. They further contended that even if Article 6 did apply, when the proceedings were taken as a whole the applicants could not be said to have been denied the right to a fair trial. In particular, they observed that the applicants did not have to overcome any evidential burden to apply to the IPT; there was scrutiny of all the relevant material, open and closed, by the IPT, which had full powers to obtain any material it considered necessary; material was only withheld where the IPT was satisfied that there were appropriate public interest and national security reasons for doing so; and finally, the IPT appointed Counsel to the Tribunal who in practice performed a similar function to that of a Special Advocate in closed material proceedings. With regard to the meeting in 2007 between MI5 and the IPT,

they advised the Court that at the meeting MI5 had indicated that, for the purposes of IPT proceedings, it would not routinely conduct searches of "reference data-bases", being databases containing information about the population generally (such as the Voter's Roll or telephone directories), for any mention of a complainant's name; instead, such searches would only be carried out if the data was "relevant or had been relied on in the course of an investigation".

505. In their third party intervention, the ENNHRI submitted that the principle of equality of arms – being a core aspect of Article 6 of the Convention – was incompatible with the exclusion of one party from a hearing in which the other participates, other than in exceptional circumstances where adequate procedural safeguards provide protection from unfairness and no disadvantage ensues.

506. To date, neither the Commission nor the Court has found that Article 6 § 1 of the Convention applies to proceedings relating to a decision to place a person under surveillance. For example, in *Klass v. Germany* the Commission found that Article 6 § 1 was not applicable either under its civil or under its criminal limb (see *Klass and Others*, cited above, §§ 57-61) and, more recently, in *Association for European Integration and Human Rights and Ekimdzhiev* (cited above, § 106) the Court "did not perceive anything in the circumstances of the case that could alter that conclusion".

507. However, the IPT has itself gone further than this Court. In its joint Ruling on Preliminary Issues of Law in the *British-Irish Rights Watch Case*, it accepted that Article 6 applied to "a person's claims under section 65(2)(a) and to his complaints under section 65(2)(b) of RIPA, as each of them involves "the determination of his civil rights' by the Tribunal within the meaning of Article 6(1)" (see paragraph 137 above). Consequently, when the matter came before the Court in *Kennedy* it did not consider it necessary to reach a conclusion on the matter, since it held that, even assuming that Article 6 § 1 applied to the proceedings in question, there had been no violation of that Article (*Kennedy*, cited above, §§ 177-179 and §§ 184-191).

508. In the present case, it is similarly unnecessary for the Court to reach any firm conclusion on the question of the applicability of Article 6 of the Convention since, for the reasons set out below, it considers that the applicants' complaint is manifestly ill-founded.

509. With regard to the applicants' general complaints concerning the procedure before the IPT, including the limitations on disclosure and the holding of public hearings in the interests of national security, the Court recalls that similar complaints were made in *Kennedy* and the Court, having considered the relevant procedural rules, concluded that in order to ensure the efficacy of the secret surveillance regime, and bearing in mind the importance of such measures to the fight against terrorism and serious crime, the restrictions on the applicant's procedural rights were both

necessary and proportionate and did not impair the very essence of his Article 6 rights (*Kennedy*, cited above, §§ 177-179 and §§ 184-191).

510. The Court sees no reason to come to a different conclusion in the present case. It has already found, in paragraphs 250-265 above, that in view of the IPT's extensive power to consider complaints concerning the wrongful interference with communications pursuant to RIPA, it was an effective remedy, available in theory and practice, which was capable of offering redress to persons complaining of both specific incidences of surveillance and the general Convention compliance of a surveillance regime. Furthermore, these extensive powers were employed in the applicants' case to ensure the fairness of the proceedings; in particular, there was scrutiny of all the relevant material, open and closed, by the IPT; material was only withheld from the applicants where the IPT was satisfied that there were appropriate public interest and national security reasons for doing so; and finally, the IPT appointed Counsel to the Tribunal to make submissions on behalf of the applicants in the closed proceedings.

511. Insofar as the applicants complain about the meeting between the IPT and the intelligence services in 2007, the Court considers that, in view of the IPT's specialist role, the fact that its members met with the services to discuss procedural matters does not, of itself, call into question its independence and impartiality. Furthermore, the applicants have not adequately explained how the 2007 meeting impacted on the fairness of their IPT proceedings in 2014 and 2015. Although the applicants appear to suggest that the resulting protocol might have affected the IPT's ability to access information held about them, the Government's explanation of the protocol (namely, that it concerned an agreement not to conduct searches of databases containing information about the population generally, such as the Voter's Roll or telephone directories, unless the data was "relevant or had been relied on in the course of an investigation") confirms that it could have had no impact on the fairness of the IPT proceedings in the present case.

512. Finally, it would appear that the error regarding the identity of the applicants whose rights were violated was an administrative mistake (see paragraph 53 above) and, as such, does not indicate any lack of rigour in the judicial process.

513. Accordingly, the Court considers that the complaint under Article 6 § 1 of the Convention must be rejected as manifestly ill-founded pursuant to Article 35 § 3 (a) of the Convention.

V. ALLEGED VIOLATION OF ARTICLE 14 OF THE CONVENTION COMBINED WITH ARTICLES 8 AND 10 OF THE CONVENTION

514. The applicants in the third of the joined cases further complained under Article 14 of the Convention, read together with Articles 8 and 10, that the section 8(4) regime was indirectly discriminatory on grounds of

nationality because persons outside the United Kingdom were disproportionately likely to have their private communications intercepted; and section 16 of RIPA provides additional safeguards only to persons known to be in the British Islands.

515. Article 14 provides as follows:

> "The enjoyment of the rights and freedoms set forth in [the] Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status."

516. However, the applicants have not substantiated their claim that persons outside the United Kingdom are disproportionately likely to have their private communications intercepted under the section 8(4) regime. First of all, although the regime targets "external communications", this is defined as "a communication sent or received outside the British Islands". This does not, therefore, exclude the interception of communications where one of the parties is in the British Islands. Secondly, and in any event, it has already been acknowledged that "internal communications" (where both the sender and receiver are in the British Islands) are frequently – and lawfully – intercepted as a by-catch of a section 8 (4) warrant.

517. Insofar as section 16 prevents intercepted material from being selected for examination according to a factor "referable to an individual who is known to be for the time being in the British Islands", any resulting difference in treatment would not be based directly on nationality or national origin, but rather on geographical location. In *Magee v. the United Kingdom*, no. 28135/95, § 50, ECHR 2000-VI the Court held that as such a difference in treatment could not be explained in terms of personal characteristics, it was not a relevant difference in treatment for the purposes of Article 14 of the Convention and did not amount to discriminatory treatment within the meaning of Article 14 of the Convention (see *Magee*, cited above, § 50).

518. In any event, the Court is of the view that any difference in treatment based on geographic location was justified. The Government have considerable powers and resources to investigate persons within the British Islands and do not have to resort to interception of their communications under a section 8(4) warrant. They do not, however, have the same powers to investigate persons outside of the British Islands.

519. Accordingly, the Court considers that the complaint under Article 14 of the Convention, read together with Articles 8 and 10, must be rejected as manifestly ill-founded pursuant to Article 35 § 3(a) of the Convention.

VI. APPLICATION OF ARTICLE 41 OF THE CONVENTION

520. Article 41 of the Convention provides:

> "If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

A. Damage

521. The applicants did not submit any claim in respect of pecuniary or non-pecuniary damage. Accordingly, the Court considers that there is no call to award them any sum on that account.

B. Costs and expenses

522. The applicants in the first and second of the joined cases made a claim for costs and expenses incurred before the Court. The applicants in the first of the joined cases claimed GBP 208,958.55 in respect of their costs and expenses; and the applicants in the second of the joined cases claimed GBP 45,127.89. The applicants in the third of the joined cases made no claim in respect of costs and expenses.

523. The Government did not comment on the sums claimed.

524. According to the Court's case-law, an applicant is entitled to the reimbursement of costs and expenses only in so far as it has been shown that these have been actually and necessarily incurred and are reasonable as to quantum. In the present case, regard being had to the documents in its possession and the above criteria, the Court considers it reasonable to award the applicants in the first of the joined cases the sum of EUR 150,000 for the proceedings before the Court; and the applicants in the second of the joined cases the sum of EUR 35,000 for the proceedings before the Court.

C. Default interest

525. The Court considers it appropriate that the default interest rate should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

FOR THESE REASONS, THE COURT:

1. *Declares*, unanimously, the complaints made by the applicants in the third of the joined cases concerning Article 6, Article 10, insofar as the applicants rely on their status as NGOs, and Article 14 inadmissible;

2. *Declares*, unanimously, the remainder of the complaints made by the applicants in the third of the joined cases admissible;

3. *Declares*, by a majority, the complaints made by the applicants in the first and second of the joined cases admissible;

4. *Holds*, by five votes to two, that there has been a violation of Article 8 of the Convention in respect of the section 8(4) regime;

5. *Holds*, by six votes to one, that there has been a violation of Article 8 of the Convention in respect of the Chapter II regime,

6. *Holds*, by five votes to two, that there has been no violation of Article 8 of the Convention in respect of the intelligence sharing regime;

7. *Holds*, by six votes to one, that, insofar as it was raised by the applicants in the second of the joined cases, there has been a violation of Article 10 of the Convention in respect of the section 8(4) regime and the Chapter II regime;

8. *Holds,* unanimously, that there is no need to examine the remaining complaints made by the applicants in the third of the joined cases under Article 10 of the Convention;

9. *Holds*, by six votes to one,
(a) that the respondent State is to pay the applicants, within three months from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, the following amounts, to be converted into the currency of the respondent State at the rate applicable at the date of settlement:
(i) to the applicants in the first of the joined cases: EUR 150,000 (one hundred and fifty thousand euros), plus any tax that may be chargeable to the applicants, in respect of costs and expenses;
(ii) to the applicants in the second of the joined cases: EUR 35,000 (thirty-five thousand euros), plus any tax that may be chargeable to the applicants, in respect of costs and expenses;
(b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amounts at a

rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points; and

10. *Dismisses*, unanimously, the remainder of the applicants' claim for just satisfaction.

Done in English, and notified in writing on 13 September 2018, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Abel Campos Registrar	Linos-Alexandre Sicilianos President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the following separate opinions are annexed to this judgment:

(a) partly concurring, partly dissenting opinion of Judge Koskelo, joined by Judge Turković; and

(b) joint partly dissenting and partly concurring opinion of Judges Pardalos and Eicke.

L.-A.S.
A.C.

APPENDIX

List of Applicants

App. No.	Applicants
58170/13	Big Brother Watch
58170/13	English PEN
58170/13	Open Rights Group
58170/13	Dr Constanze Kurz
62322/14	Bureau of Investigative Journalism
62322/14	Alice Ross
24960/15	Amnesty International Limited
24960/15	Bytes For All
24960/15	The National Council for Civil Liberties ("Liberty")
24960/15	Privacy International
24960/15	The American Civil Liberties Union
24960/15	The Canadian Civil Liberties Association
24960/15	The Egyptian Initiative For Personal Rights
24960/15	The Hungarian Civil Liberties Union
24960/15	The Irish Council For Civil Liberties Limited
24960/15	The Legal Resources Centre

PARTLY CONCURRING, PARTLY DISSENTING OPINION OF JUDGE KOSKELO, JOINED BY JUDGE TURKOVIĆ

1. I have voted, and agree, with the majority as regards points 1 to 3 of the operative provisions of the judgment, which concern the admissibility of the complaints. I have also joined the majority in finding a violation of Article 8 in respect of both the section 8(4) regime and the Chapter II regime. As regards the section 8(4) regime, however, I am not able in all respects to subscribe to the reasons given by the majority. As far as the intelligence sharing regime is concerned, unlike the majority, I have voted for finding a violation of Article 8.

I. The RIPA section 8(4) regime

2. The present case concerns legislation providing for secret surveillance, by means of bulk interception, of electronic communications which qualify as "external" (for an understanding of the concept of "external" communications see paragraphs 69-71 of the judgment). It is important to note that this type of secret surveillance of communications is not limited to certain already known or identified targets but is aimed at the discovery of threats and hitherto unknown or unidentified targets which might be responsible for threats (see paragraph 284 of the judgment). The relevant threats are broadly framed and comprise threats to national security or to the economic well-being of the country as well as threats arising from serious crime (see §§ 57-59).

3. It is obvious that such an activity – an untargeted surveillance of external communications with a view to discovering and exploring a wide range of threats – by its very nature takes on a potentially vast scope, and involves enormous risks of abuse. The safeguards against those risks, and the standards which under the Convention should apply in this regard, therefore raise questions of the highest importance. I am not convinced, in the light of present-day circumstances, that reliance on the Court's existing case-law provides an adequate approach to the kind of surveillance regimes like the one we are dealing with here. A more thorough reconsideration would be called for. I acknowledge that this would be a task for the Court's Grand Chamber. I will only raise some concerns which, in my view, require attention in this regard.

(i) The context of earlier case-law

4. Apart from the recent Chamber judgment in *Centrum för Rättvisa v. Sweden* (no. 35252/08, 19 June 2018), which is not yet final, the Court's case-law has not dealt with the present kind of surveillance but with regimes which, as a matter of either law or fact, have been narrower in scope. Furthermore, in the light of current developments, I consider that reliance

on the line of existing case-law is no longer an adequate basis for assessing the standards which under the Convention should govern this particular domain.

5. The Court's case-law on secret surveillance of communications essentially dates back to *Klass and Others v. Germany* (cited in the judgment) which was decided by the Plenary Court four decades ago, and the admissibility decision in *Weber and Saravia v. Germany* (also cited in the judgment), which concerned an amended version of the same German legislation and was decided twelve years ago, in response to a complaint lodged in the year 2000.

6. As the Court noted in *Klass and Others*, the German legislation then at issue (the G 10) laid down a series of limitative conditions which had to be satisfied before a surveillance measure could be imposed. Thus, the permissible restrictive measures were *confined to cases in which there were factual indications for suspecting a person of planning, committing or having committed certain serious criminal acts*; measures could only be ordered if the establishment of the facts by another method was without any prospect of success or considerably more difficult; even then, the surveillance could cover *only the specific suspect or his presumed "contact-persons"*. Thus, the Court observed, "*so-called exploratory or general surveillance [was] not permitted by the contested legislation*" (see *Klass and Others*, § 51).

7. In this regard, the RIPA section 8(4) regime which is at issue in the present case is different from that in *Klass and Others* in that the section 8(4) regime does encompass what the Court then referred to as "exploratory" surveillance and which in fact constitutes an essential and critical feature of this particular regime. Consequently, the scope and purpose of the surveillance regime now at issue is wider than that addressed in *Klass and Others*.

8. In *Weber and Saravia*, the complaint concerned a revised version, adopted in 1994, of the German G 10, whereby the scope of permissible surveillance was extended to cover the monitoring of international wireless telecommunications (see *Weber and Saravia*, § 88) in order to allow a "strategic surveillance" of such communications by means of catchwords. According to the Government's submissions in that case, at the relevant time merely some ten per cent of all telecommunications were conducted by wireless means, and thus potentially subject to monitoring. In practice, monitoring was restricted to a limited number of foreign countries. The telephone connections of the State's own (i.e. German) nationals living abroad could not be monitored directly. The identity of persons telecommunicating could only be uncovered in rare cases in which a catchword had been used (ibid., § 110).

9. The surveillance regime at issue in *Weber and Saravia* covered international wireless communications traffic, i.e. traffic transmitted via

microwave or satellite, the latter operating through a survey of the downlink to Germany. Line-bound international communications were not subject to monitoring except where the risk of a war of aggression was concerned.

10. It is noteworthy that at the time of the surveillance regime which gave rise to the complaint in *Weber and Saravia*, strategic monitoring was mainly carried out on telephone, telex and fax communications. In those days, surveillance did not extend to email communications (see the judgment of the Federal Constitutional Court of 14 July 1999, 1BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95, Rn 230, according to which, at the time of the hearing of the case in 1999, an expansion of strategic monitoring to email communications was only being planned for the future). One significant feature of communications by email, apart from the fact that nowadays they are so common, is that the identity of both the sender and recipient is usually directly available. Furthermore, many currently used means of communication or access to information through the Internet were only at embryonic stages at the time of the domestic complaint in *Weber and Saravia*.

(ii) The context of the present case

11. My point with the remarks above is to draw attention to the factual environment against the background of which those earlier cases were adjudicated, and the dramatic changes that have occurred since. The applicants have indeed referred to the technological "sea change" which has taken place.

12. What is important to note in this regard is that the technological "sea change" has had a twofold impact. On the one hand, technological developments have advanced the means by which surveillance of communications can be carried out. On the other hand, new technologies have revolutionised the ways in which people communicate, access, use and share information. That change is deeper than just a matter of volume. The digital age has in some respects transformed people's lifestyles.

13. As a result of these changes, the potential exposure nowadays of a vast range of communications and other online activities to secret surveillance is far greater than before. In the wake of such developments, the potential risks of abuse arising from such surveillance have increased as well. Thus, the factual context in which "exploratory" or "strategic" secret surveillance operates is dramatically different from the circumstances that still prevailed a couple of decades ago, when the *Weber and Saravia* application was lodged, let alone four decades ago, when *Klass and Others* was decided. In the light of such changes, it is problematic and troubling to approach the question of the necessary safeguards against abuse simply by applying standards that were considered sufficient under significantly or even essentially different factual circumstances.

14. Furthermore, the "sea change" in terms of technologies and digitalised lifestyles is not the only development to be taken into consideration. The threats on account of which surveillance of communications is considered necessary have also changed. In this regard, too, the picture is twofold. One the one hand, for instance, there have been real and well-known aggravations in the risks of international terrorism. On the other, there is also increasing evidence of how various threats can be invoked, rightly or wrongly, in order to justify measures that entail restrictions on individual rights and freedoms. The notion of terrorism, for instance, may sometimes be used quite loosely and opportunistically in a desire to legitimise interferences with such rights and freedoms. Especially where secret surveillance is conducted in order to discover and explore broadly formulated threats such as those to national security or the nation's economic well-being, the need for real safeguards through independent control and review is obvious.

15. There is yet another "sea change" calling for heightened attention in the assessment of the necessary standards in the context of secret surveillance of communications. It is the degradation of respect for democratic standards and the rule of law of which there is increasing evidence in a number of States. While I am not suggesting that the present respondent State is a case in point in this regard, the Convention standards must nevertheless be considered in the light of the fact that such developments testify to the actual or potential fragility of safeguards, institutional arrangements and the underlying assumptions that in ideal circumstances might appear adequate in order to minimise the risks of abuse. In fact, the same threats that are invoked to justify secret surveillance may also serve to reinforce tendencies toward a weakening of the checks and balances which underpin adherence to the rule of law and democratic governance.

(iii) Concerns

16. In line with the majority, I agree that the Contracting States must enjoy a wide margin of appreciation in determining whether the protection of national security requires the kind of surveillance of communications which is at issue in the present case (paragraph 314 of the present judgment). However, given the high risks of abuse, which at worst may undermine not only individual rights and freedoms but democracy and the rule of law more generally, the margin must be narrow when it comes to the necessary safeguards against abuse.

17. Under the impugned legislation, one of the striking features is that all of the supervisory powers entrusted to authorities with independence from the executive are of an *ex post* nature. Another striking feature is that not only are the general protective aims of the legislation very broadly framed, but also the specific authorisations (warrants and certificates) issued

by the Secretary of State appear to be formulated in very broad and general terms (see paragraphs 156 and 342). Furthermore, the concrete search and selection criteria which are applied to filter intercepted communications for reading of their content are determined by the analysts conducting the surveillance (see paragraphs 157, 340 and 345-46 of the present judgment). As indicated by the domestic findings, the latter are not even subject to any meaningful subsequent oversight by independent bodies (see paragraphs 157 and 340).

18. Ever since *Klass and Others*, the Court has indeed held that in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse (see *Klass and Others*, §§ 49-50). This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law (ibid., § 50).

19. As discussed above, in the light of the changes in both the nature and scope of surveillance and in the prevailing factual realities, the circumstances have indeed evolved in such a way and to such an extent that I find it difficult to accept that the adequacy of safeguards should nevertheless be assessed simply by relying on the case-law that has arisen under different legal and factual framework conditions.

20. In particular, given the present overall context, I question the approach according to which prior independent control by a judicial authority should not be a necessary requirement in the system of safeguards.

21. Already in *Klass and Others*, when considering the initial stage of control, the Court stated that, in a field where abuse was potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it was in principle desirable to entrust supervisory control to a judge (see *Klass and Others*, § 56). Under the G 10 legislation, judicial control was replaced by an initial control effected by an official qualified for judicial office and by the control provided by the Parliamentary Board and the G 10 Commission. In that case the Court concluded that, having regard to the nature of the supervisory and other safeguards provided for by the G 10, the exclusion of judicial control did not exceed the limits of what might be deemed necessary in a democratic society. The Court noted that the Parliamentary Board and the G 10 Commission were independent of the authorities carrying out the surveillance and vested with sufficient powers and competence to exercise an effective and continuous control. Furthermore, the democratic character was reflected in the balanced membership of the Parliamentary Board, on which the opposition was represented and was thus able to participate in the

control of the measures ordered by the competent Minister, who was accountable to the Bundestag. The Court found that the two supervisory bodies could, in the circumstances of the case, be regarded as enjoying sufficient independence to give an objective ruling (ibid.).

22. As indicated above, in my view the legal and factual circumstances of that case, which go back four decades, cannot be considered comparable to the situation now under consideration. It is somewhat striking that in *Weber*, despite the important changes in the legislative and factual framework, the Court succinctly stated that it saw no reason to reconsider the conclusion in *Klass and Others* (see *Weber and Saravia*, § 117). In any event, in the light of the circumstances prevailing at the present time, such reconsideration seems to me to be indispensable.

23. Where, as in the present case, the interception (as a matter of technical necessity) encompasses vast volumes of communications traffic in an indiscriminate manner, without being linked to any kind of prior elements of suspicion related to the threats by reason of which the surveillance is conducted, everything in terms of the protection of individuals and their rights depends on whether and how the subsequent stages of the treatment of the intercepted communications provide effective and reliable safeguards for those rights, and against any abuse of the surveillance. Under such circumstances, given the potential intrusiveness of the surveillance and the abundant risks of abuse, I consider that it cannot be appropriate that all the *ex ante* safeguards remain in the hands of the executive. I think the applicants are right to argue that there is a need for an "updating" of the standards as regards prior independent judicial authorisation. It seems to me to be important that the authorities of the executive branch should be required to explain and justify before an independent judicial authority the grounds on which a particular surveillance should be authorised, and to account for the search criteria on the basis of which the intercepted communications will be filtered and selected for a review of their content.

24. In this respect, I am not convinced by the arguments advanced by the majority in support of the position that prior judicial control is unnecessary (paragraphs 318-20). The majority acknowledge that judicial authorisation is not inherently incompatible with the effective functioning of bulk interception (paragraph 318). Indeed, the recent case of *Centrum för Rättvisa v. Sweden* (cited above) offers an illustration, as it deals with Swedish legislation under which prior judicial authorisation is required.

25. The main argument against imposing such a requirement appears to be that it would not entail a sufficient safeguard, and that even in the absence of prior judicial authorisation the existence of independent oversight by the IPT and the Interception of Communications Commissioner provide adequate safeguards against abuse. In my view, it is obvious that prior judicial authorisation cannot in itself be sufficient and

that further, robust safeguards such as those in place in the UK are indeed required. However, the fact that a given safeguard would not be sufficient is not enough to support a conclusion that it should not be considered necessary. In my opinion, it is quite essential to have in place an adequate system of safeguards, including controls exercised by independent bodies, both *ex ante* and *ex post*.

26. While the safeguards *ex post* that are provided for in the UK legislation and practice appear to set a good model in this domain, this does not in my view suffice to remedy the fact that the authorisation and implementation of the surveillance are wholly in the hands of the executive authorities, without any independent control *ex ante*. In this respect, the system of safeguards is even weaker than that considered by the Court in both *Klass and Others* and *Weber and Saravia,* in that under the German G 10 regime, although the surveillance was not subject to prior authorisation by a court, it had to be authorised by the G 10 Commission (see *Weber and Saravia*, cited above, § 115), which was not an executive branch body (ibid., § 25). Moreover, according to the judgment of the Federal Constitutional Court of 14 July 1999 (cited above, Rn 87), a list of search concepts was part of each restriction order, whereas in the present case it has transpired that the search and selection criteria are determined by the analysts operating the surveillance and are not subject to any prior supervision, nor any meaningful subsequent oversight (see paragraphs 157, 340 and 345-46 of the present judgment).

27. In sum, what we have before us now is a regime of secret surveillance, the reach of which under the prevailing factual circumstances is unprecedented, and under which a very wide operational latitude is left to the services operating the surveillance, without any independent *ex ante* control or constraint, and under which the search and selection criteria are not even *ex post* subject to any robust independent control. I find such a situation highly problematic. An independent *ex ante* control is all the more important because of the secret nature of the surveillance, which in practice reduces the possibility that individuals will have recourse to the safeguards available *ex post*.

28. I also consider that the remarks made by the majority in paragraph 319 of the judgment are not capable of supporting a conclusion according to which prior independent judicial authorisation should not be required. Rather, the argument that even judicial scrutiny may fail its function serves to underline the crucial importance which attaches to the requirement that such control must have effective guarantees of independence, in order to meet the proper standards of the necessary safeguards.

29. In short, while I agree with the conclusions set out in paragraph 387 of the judgment, I do not consider those shortcomings to be the only ones that justify a finding of a violation of Article 8 in the present case. In

particular, taking into account the present legal and factual context, I do not believe that the necessary safeguards in the circumstances of surveillance based on the bulk interception of communications can be sufficient without including an independent *ex ante* judicial control. The position according to which prior judicial control of authorisations for secret surveillance of communications was a desirable but not a necessary safeguard stems from *Klass and Others* which, firstly, concerned a more limited surveillance regime than the one now at issue and did not permit "exploratory surveillance" at all, and which, secondly, was decided four decades ago against the backdrop of factual circumstances that in many relevant respects were different from those prevailing today. That position was later, in *Weber and Saravia*, carried over to a surveillance regime which did have more similarities with the RIPA section 8(4) regime but nevertheless operated in conditions very different from those prevailing in the modern digitalised societies. For the reasons outlined above, that position should, in my view, no longer be maintained by the Court.

II. The intelligence-sharing regime

30. It is easy to agree with the principle that any arrangement under which intelligence from intercepted communications is obtained via foreign intelligence services, whether on the basis of requests to carry out such interception or to convey its results, should not be allowed to entail a circumvention of the safeguards which must be in place for any surveillance by domestic authorities (see paragraphs 216, 423 and 447). Indeed, any other approach would be implausible.

31. On this basis I consider, in sum, that the shortcomings referred to above in the context of the section 8(4) regime also attach to the intelligence-sharing regime (see paragraphs 109 and 428-29). I therefore conclude that the safeguards have not been adequate and that there has been a violation of Article 8 in respect of this regime also.

JOINT PARTLY DISSENTING AND PARTLY CONCURRING OPINION OF JUDGES PARDALOS AND EICKE

Introduction

1. For the reasons set out in more detail below, we are unfortunately, not able to agree with the majority in relation to two aspects of the judgment in this case; namely

(a) that the applicants in the first and second of the joined cases had shown "special circumstances absolving them from the requirement to exhaust" domestic remedies by first bringing proceedings before the IPT (§§ 266-268 and operative part § 3; "admissibility"); and

(b) that there has been a breach of Article 8 of the Convention in respect of the section 8(4) regime (§ 388 and operative part § 4; "the section 8(4) regime").

2. In relation to the latter issue our position is reinforced by the contrast between the conclusions reached by the majority in this case and that reached in the judgment in *Centrum För Rättvisa v. Sweden*, no. 35252/08 (not yet final); a judgment adopted by the Third Section of this Court on 19 June 2018, a mere two weeks before the final deliberations in this case. In that case, the Court concluded, unanimously, that, despite having identified "some areas where there is scope for improvement" (§ 180) and "making an overall assessment and having regard to the margin of appreciation enjoyed by the national authorities in protecting national security" (§ 181), the Swedish system of signals intelligence provided adequate and sufficient guarantees against arbitrariness and the risk of abuse; as a consequence, it was held that the relevant legislation met the "quality of law" requirement, that the "interference" established could be considered as being "necessary in a democratic society" and that the structure and operation of the system were proportionate to the aim sought to be achieved.

3. That said, we agree both with:

(a) the underlying general principles identified by the Court both in this case and in *Centrum För Rättvisa* to be applied in relation to these aspects of the case; as well as

(b) the conclusion of the majority in this case that, for the reasons given in the judgment, there has been no breach of Article 8 of the Convention in relation to the intelligence sharing regime (§§ 447-448 and operative part § 6) and that there is no need to examine the remaining complaints made by the applicants in the third of the joined cases under Article 10 of the Convention.

4. In relation to the findings that there has been a breach of the Convention in relation to the Chapter II regime (§§ 468 and 500, operative part §§ 5 and 7) as well as the conclusions under Article 41 of the Convention (operative part § 9), one of us (Judge Pardalos) considered that her conclusion on the admissibility of the first and second of the joined cases invariably determined the related substantive issues against the applicants in those cases. By contrast, Judge Eicke considered that, the Court having decided that the first and second cases were, contrary to his view, admissible he was required, as a member of that Court, to go on and decide those cases on the merits by reference to the evidence and pleadings before the Court.

Admissibility

5. As indicated above, we agree with the majority that, for the reasons they give, the IPT is and has been an effective remedy "since Kennedy was decided in 2010" (§ 268); i.e. a remedy which is "available in theory and practice" and "capable of offering redress to applicants complaining of both specific incidences of surveillance and the general Convention compliance of surveillance regimes" (§ 265). Consequently, applicants before this Court will be expected to have exhausted this domestic remedy before the Court has jurisdiction to entertain their application under Article 35 § 1 of the Convention.

6. In addition to the purely legal point that, under Article 35 § 1, the Court "may only deal with the matter after all domestic remedies have been exhausted", we would underline what the majority says in § 256 about the invaluable assistance derived by the Court, in examining a complaint before it, from the "elucidatory" role played by the domestic courts (in this case the IPT) both generally as well as in the specific context of considering the compliance of a secret surveillance regime with the Convention.

7. For the reasons set out below, however, we disagree with the conclusion reached by the majority (§ 268) that there existed, in this case, "special circumstances" absolving the applicants in the first and second of the joined cases from satisfying this requirement.

8. Firstly, as the majority implicitly accepts (§ 267), the case of *Kennedy* is clearly distinguishable on its facts from the present case. After all, the applicant in that case had already brought a specific complaint about the section 8(1) regime before the IPT before applying to this Court. Consequently, unlike the applicants in the first and second of these joined cases, Mr Kennedy was not inviting the Court to consider his general complaint entirely *in abstracto*. Furthermore, in its judgment in that case, the Court considered it "important" that his challenge was (consequently) exclusively a challenge to primary legislation. By contrast, in the present cases the scope of each of the regimes complained of (bulk interception,

intelligence sharing and the acquisition of communications data) is significantly broader than that of the section 8(1) regime, and the applicants' complaints concern not only primary legislation, but the overall legal framework governing those regimes (including the alleged absence of any relevant arrangements or other safeguards). Consideration of the broader legal framework necessarily requires an examination of both RIPA and the relevant Codes of Practice, together with any "below the waterline" arrangements and/or safeguards. In view of the much broader scope of both their complaints and the impugned regimes, none of which had been the subject of any examination by the IPT, it should have been evident to the applicants in the first and second of the joined cases – who were, at all times, represented by experienced counsel – that, unlike *Kennedy*, this was a case in which the general operation of these regimes required further elucidation, and in which the IPT, on account if its "extensive powers ... to investigate complaints before it and to access confidential information" would have been capable of providing a remedy.

9. There is, therefore, also no basis for any suggestion that our approach seeks, in any way, to overturn or "disapply" the Court's unanimous ruling in *Kennedy*. The simple fact is that, in our view, the two are clearly and obviously distinguishable.

10. Secondly, the first applicant, was clearly informed by the Government, in their response to the letter before action of 26 July 2013 (§ 19), that their complaints could be raised in the IPT, a court established specifically to hear allegations by citizens of wrongful interference with their communications as a result of conduct covered by that Act and a court endowed with exclusive jurisdiction to investigate any complaint that a person's communications have been intercepted and, where interception has occurred, to examine the authority for such interception. This letter was, of course, sent at around the same time as the ten human rights organisations which are the applicants in the third of the joined cases, no doubt recognising the need to have exhausted existing effective domestic remedies before applying to this Court, lodged their complaints before the IPT (June to December 2013; § 21). It was also four years after the UK Supreme Court, in its judgment in *R (on the application of A) v B* [2009] UKSC 12, had confirmed the exclusive jurisdiction of the IPT and its ability, as demonstrated by its decisions in *Kennedy* (IPT/01/62 & 77) and *The British-Irish Rights Watch and others v Security Service, GCHQ and the SIS* (IPT/01/77), to adjust the procedures before it as necessary so as to ensure that disputes before it can be determined justly.

11. Thirdly and in any event, even if, contrary to our view, the applicants in the first and second of the joined cases would have been entitled to rely on *Kennedy* at the time they lodged their applications with the Court they nevertheless accepted before this Court (§ 241), by reference to the judgment in *Campbell and Fell v. the United Kingdom*, 28 June 1984,

§§ 62-63, Series A no. 80, that in light of any finding by the Court to the effect that the IPT is an effective remedy, they would now be required to go back and exhaust unless it would be unjust to require them to do so. As these applicants' complaints concern the general operation of the impugned regimes, rather than specific complaints about an interference with their rights under the Convention, they would still be entitled to raise them before the IPT now.

12. Many of the complaints advanced in the first and second of the joined applications (including, in particular, all of those relating to the Chapter II regime, the sharing of non-intercept material with foreign governments and the lack of protection for confidential journalistic material and journalistic sources under the section 8(4) regime) were not addressed in the *Liberty* proceedings and have not yet been determined by the IPT. Consequently, there is no reason to doubt that if the applicants were now to raise those complaints before the IPT, they would have "a reasonable prospect of success". In fact, in respect of the Chapter II complaint it may be thought that they would have a more than reasonable prospect of success. After all, as the majority records in § 463 of the judgment, the Government, in response to a challenge brought by Liberty, recently conceded that Part 4 of the IPA (which included a power to issue "retention notices" to telecommunications operators requiring the retention of data) was incompatible with fundamental rights in EU law: *R (The National Council for Civil Liberties (Liberty)) v Secretary of State for the Home Department & Anor* [2018] EWHC 975 (Admin). As Chapter II of RIPA, like Part 4 of the IPA, permits access to data for the purpose of combating crime (as opposed to "serious crime"), this concession lead the majority to find a violation of Article 8 of the Convention in relation to the Chapter II regime (§ 467) which would suggest that the applicants had a strong basis for challenging, at the domestic level, the compliance of the Chapter II regime with EU law and, indeed, the Convention.

13. The same could not necessarily be said about those complaints raised by the first and/or second of the joined cases which were determined by the IPT in the *Liberty* proceedings; however, those issues were, of course, also raised by the applicants in the third of the joined cases and would therefore (and in fact have been) considered and determined by the Court on its merits.

14. As a result, and in clear contrast with the ultimate conclusion in *Campbell and Fell*, there is here therefore no evidence to suggest that "it would be unjust now to find these complaints inadmissible for failure to exhaust domestic remedies" (*ibid.* at § 63). Consequently, in our view, both the requirements of Article 35 § 5 of the Convention as well as the application of the principle of subsidiarity, in fact, required such a finding.

15. The point made in the judgment about the fundamental importance of the "elucidatory" role of the domestic courts is further underlined by the

complaint made in relation to the Chapter II regime. After all, as the judgment records in § 451, in both their application to the Court and their initial observations, the applicants in the second of the joined cases had incorrectly referred to the Chapter II regime as a regime for the interception of communications data; rather than a regime which permits certain public authorities to acquire communications data from Communications Service Providers ("CSPs"). This "fundamental legal misunderstanding" led the Government to submit *inter alia* that the applicants had put forward no factual basis whatsoever for concluding that their communications were acquired in this way, and that they did not contend that they had been affected, either directly or indirectly, by the regime.

16. As noted above, the Court's conclusion on the Chapter II regime was, of course, ultimately based on the concession by the Government in *R (The National Council for Civil Liberties (Liberty)) v Secretary of State for the Home Department & Anor* [2018] EWHC 975 (Admin) which enabled the majority to find that the equivalent language in the Chapter II regime was "not in accordance with the law" within the meaning of Article 8 of the Convention (§ 467). However, had that not been the case, this Court would have been confronted with the task of considering in detail whether the regime's attendant safeguards were sufficient to satisfy the requirements of the Convention; and that (1) on the basis of a case initially advanced on the basis of a "fundamental legal misunderstanding" about the nature of the regime, (2) without any assistance or findings by the IPT in relation to what the attendant safeguards, both above and below the waterline, in fact were and/or (3) any reasoned conclusion by the IPT as to whether or not they satisfied the requirements of Article 8 (or could be made to satisfy the requirements of Article 8 by means of further disclosure akin to that ordered on 9 October 2014 in the proceedings brought by the applicants in the third of the joined applications). This would plainly have been a wholly undesirable state of affairs.

The section 8(4) regime

17. As indicated above, there is much in the judgment of the majority we agree with.

18. Firstly, we agree with the majority (as well as with the unanimous judgment in *Centrum För Rättvisa*) in relation to the relevant general principles as set out in the judgment. In particular we agree with the affirmation by the majority (as well as the judgment in *Centrum För Rättvisa* and the report by the Venice Commission) that while the Court has considered prior judicial authorisation to be an important safeguard, and perhaps even "best practice", it has also repeatedly confirmed that, by itself, such prior judicial authorisation is neither necessary nor sufficient to ensure compliance with Article 8 of the Convention (§ 320).

19. Secondly, we also agree with the majority in identifying as potential shortcomings (or, to use the language in *Centrum För Rättvisa* "areas where there is scope for improvement") in the operation of the section 8(4) regime "the lack of oversight of the entire selection process, including the selection of bearers for interception, the selectors and search criteria for filtering intercepted communications, and the selection of material for examination by an analyst; and secondly, the absence of any real safeguards applicable to the selection of related communications data for examination" (§ 387).

20. Finally, we agree with the majority as to the correct approach to be applied when considering whether the system under review satisfied the requirement of being "necessary in a democratic society" under Article 8 § 2 of the Convention, namely that:

> "... regard must be had to the actual operation of the system of interception, including the checks and balances on the exercise of power, and the existence or absence of any evidence of actual abuse (see Association for European Integration and Human Rights and Ekimdzhiev, cited above, § 92) (§ 320)
>
> ... it must principally have regard to the actual operation of a system of interception as a whole, including the checks and balances on the exercise of power, and the existence (or absence) of any evidence of actual abuse (...), such as the authorising of secret surveillance measures haphazardly, irregularly or without due and proper consideration (see Roman Zakharov, cited above, § 267) (§ 377)."

21. Where we disagree is (again) in the application of that approach to the system under review.

22. Before setting out in little more detail the basis for our disagreement we note in passing that this Court's underlying approach appears to be in clear contrast to the approach taken by the CJEU in *Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources and Others and Settinger and Others* (Cases C-293/12 and C-594/12) and *Secretary of State for the Home Department v. Watson and Others* (C-698/15). In the former case, the CJEU was considering the validity of the Data Retention Directive, and in the latter, the validity of domestic legislation containing the same provisions as that directive. While its focus was on the retention of data by CSPs, it also considered the question of access to retained data by the national authorities. In doing so, it indicated that access should be limited to what was strictly necessary for the objective pursued and, where that objective was fighting crime, it should be restricted to fighting serious crime. It further suggested that access should be subject to prior review by a court or independent administrative authority, and that there should be a requirement that the data concerned be retained within the European Union. Therefore, while there is some similarity in the language used by the two courts, the CJEU appears to have adopted a more prescriptive approach as regards the safeguards it considers necessary. This may be due to the fact that in both cases it was considering the rights guaranteed by reference to Articles 7 (Respect for private and family life) and 8 (Protection of personal

data) of the Charter of Fundamental Rights. However, while in *Watson* the CJEU declined to state whether the protection provided by Articles 7 and 8 of the Charter was wider than that afforded by Article 8 of the Convention, we can but note that, on the one hand, Article 52 § 3 of the Charter of Fundamental Rights, while recognising the ability of EU law providing more extensive protection, is clearly expressed by reference to "rights" guaranteed by the Convention (rather than "Articles") corresponding to "rights" contained in the Charter and that, on the other hand, this Court has, at least since the 1978 judgment of the Plenary Court in *Klass and Others v. Germany*, Series A no. 28, consistently protected the right to the protection of personal data under Article 8 of the Convention. In any event, in *Ben Faiza v. France*, no. 31446/12, 8 February 2018, which was decided one year after *Watson*, and four years after *Digital Rights Ireland*, this Court did not follow the CJEU's approach, preferring instead to follow its well-established approach and to review the impugned regime as a whole in order to evaluate the adequacy of the available safeguards.

23. In any event, applying this Court's well-established approach, it is in our view, clear from the (in the context of secret surveillance cases unusually) extensive and detailed (publicly available) evidence in relation to the operation of the section 8(4) regime (summarised over some 35 pages in the judgment) that, despite the identified areas where there is scope for improvement, these are not, in themselves, sufficiently significant to justify the conclusion that "the section 8(4) regime does not meet the 'quality of law' requirement and is incapable of keeping the 'interference' to what is 'necessary in a democratic society'" (§ 388). On the contrary, adopting the approach of this Court in *Centrum För Rättvisa*, § 181, it is clear in our view that, making an overall assessment and having regard to the margin of appreciation enjoyed by the national authorities in protecting national security, the section 8(4) regime does provide adequate and sufficient guarantees against arbitrariness and the risk of abuse. As a result, we concluded that the relevant legislation meets the "quality of law" requirement and the "interference" established can be considered as being "necessary in a democratic society" and that there was, therefore, no violation of Article 8 of the Convention.

24. In this context, the contrast to the judgment in *Centrum För Rättvisa* is instructive. After all, in that case the Court applied the same general principles to the Swedish bulk interception regime and concluded, unanimously, that there was no breach of Article 8 of the Convention. Conscious of the difficulty – at times – in making detailed meaningful comparisons between different interception regimes, it is nevertheless noteworthy that the regime under consideration in that case, while equipped with judicial prior authorisation:

(a) was completely shrouded in secrecy with the Court having little meaningful information at all either about the actual generic operation of

the system (including the actual operation of the Foreign Intelligence Court ("FIC") itself) or the impact of the system on and/or operation of safeguards in relation to any individual;

(b) provided that, in principle, the FIC should hold public hearings but found that there has never been a public hearing, all decisions are confidential and no information is disclosed to the public about the number of hearings, the number of permits granted or rejected, the reasoning of the court's decisions or the amount or type of search terms being used. While the FIC is assisted by the "privacy protection representative" whose role it is to protect the "interests of the general public" he or she does not appear on behalf of or represent the interests of any affected individual. Furthermore, the privacy protection representative cannot appeal against a decision by the FIC or "report any perceived irregularities to the supervisory bodies";

(c) was concerned with interception by the National Defence Radio Establishment ("FRA") on behalf of, and which, therefore, required communication of the intercept material to, a much wider group "clients" ("the Government, the Government Offices, the Armed Forces and, as from January 2013, the Security Police and the National Operative Department of the Police Authority");

(d) provided for authorisation of interception for a greater number (eight) of "purposes" ("1) external military threats to the country, 2) conditions for Swedish participation in international peacekeeping or humanitarian missions or threats to the safety of Swedish interests in the performance of such operations, 3) strategic circumstances concerning international terrorism or other serious cross-border crimes that may threaten essential national interests, 4) the development and proliferation of weapons of mass destruction, military equipment and other similar specified products, 5) serious external threats to society's infrastructure, 6) foreign conflicts with consequences for international security, 7) foreign intelligence operations against Swedish interests, and 8) the actions or intentions of a foreign power that are of substantial importance for Swedish foreign, security or defence policy");

(e) had similar difficulties to those identified in relation to the UK regime to separate out non-external communications between a sender and receiver within the respective State at the point of collection;

(f) allows for the communication of intercept product not only to other states but also to "international organisations" (not further defined) where that is "not prevented by secrecy and if necessary for the FRA to perform its activities within international defence and security cooperation" and "it is beneficial for the Swedish government or Sweden's comprehensive defence strategy" and without any provision requiring the third country/international organisation recipient to protect

the data with the same or similar safeguards as those applicable internally; and

(g) provided for an obligation to notify the subject of an intercept after the event; an obligation which, however, "had never been used by the FRA, due to secrecy.

25. Considering the accepted difficulty in making a meaningful comparison between two or more distinct interception regime together with the different conclusions reached by this Court at about the same time, in our view, further underlines the importance of the Court adopting an approach of asking whether, taking "an overall assessment and having regard to the margin of appreciation enjoyed by the national authorities in protecting national security" the system adopted provides adequate and sufficient guarantees against arbitrariness and the risk of abuse, even if there may be individual aspects of any system which might be capable of being altered or improved. Such an approach properly reflects the role of the Convention, which is to set down "minimum standards" that can be applied across all Member States. Provided that – following an overall assessment – the Court finds that a system for bulk interception provides adequate and sufficient guarantees against arbitrariness and abuse, in view of the very different regimes in operation in different States, it will not be appropriate for it to be too prescriptive about the way in which those regimes should operate (although it may, as it did both in *Centrum För Rättvisa* and in this case, identify those aspects of the regime which could be improved upon). Applying this approach to the Court's supervisory jurisdiction in the present case (as it was in *Centrum För Rättvisa*), the Court should have given due weight to the fact that the domestic courts and authorities have subjected both the UK system as a whole as well as the individual complaints at issue to detailed and extensive scrutiny by express reference to the Convention standards and this Court's case law and should have found that there was, here, no breach of Article 8 of the Convention.

Post Scriptum

26. Since the adoption of this judgment on 3 July 2018, the IPT has handed down yet another judgment in relation to another, unrelated, aspect of the UK's surveillance regime: *Privacy International v Secretary of State for Foreign and Commonwealth Affairs (Rev 1)* [2018] UKIPTrib IPT_15_110_CH (23 July 2018). For obvious reasons this judgment was not available for consideration by the Court when it reached its conclusions on the question of exhaustion of domestic remedies (and we have heard no submissions on it). That said, it seems to us that this careful and detailed judgment provides yet further support (if any was necessary) that, in principle, the IPT is an effective remedy for the purposes of Article 35 § 1

of the Convention which applicants will be required to have exhausted before this Court has jurisdiction to entertain their application.

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

Plaintiff's Exhibit 24



NSA Director of Civil Liberties and Privacy Office Report

NSA's Implementation of Foreign Intelligence Surveillance Act Section 702

April 16, 2014

National Security Agency, Civil Liberties and Privacy Office
Report
NSA's Implementation of Foreign Intelligence Surveillance Act Section 702

April 16, 2014

INTRODUCTION

This report was prepared by the National Security Agency (NSA) Civil Liberties and Privacy Office as part of its responsibilities to enhance communications and transparency with the public and stakeholders. Its Director is the primary advisor to the Director of NSA when it comes to matters of civil liberties and privacy. Created in January 2014, the Office is also charged with ensuring that civil liberties and privacy protection are integrated into NSA activities. The intent of this paper is to help build a common understanding that can serve as a foundation for future discussions about the existing civil liberties and privacy protections.

The mission of NSA is to make the nation safer by providing policy makers and military commanders with timely foreign intelligence and by protecting national security information networks. NSA collects foreign intelligence based on requirements from the President, his national security team, and their staffs through the National Intelligence Priorities Framework. NSA fulfills these national foreign intelligence requirements through the collection, processing, and analysis of communications or other data, passed or accessible by radio, wire or other electronic means.

NSA's authority to conduct signals intelligence collection for foreign intelligence and counterintelligence purposes is provided primarily by Section 1.7(c)(1) of Executive Order 12333, as amended. The execution of NSA's signals intelligence mission must be conducted in conformity with the Fourth Amendment. This includes NSA's acquisition of communications to which a U.S. person is a party under circumstances in which the U.S. person has a reasonable expectation of privacy. The Foreign Intelligence Surveillance Act of 1978 (FISA) further regulates certain types of foreign intelligence collection, including that which occurs with compelled assistance from U.S. communications providers.

This Report describes one way in which NSA meets these responsibilities while using Section 702 of FISA, as amended by the FISA Amendments Act of 2008. Although multiple federal agencies participate in Section 702 collection, this paper describes the process by which NSA obtains, uses, shares, and retains communications of foreign intelligence value pursuant to Section 702. It also describes existing privacy and civil liberties protections built into the process.

The NSA Civil Liberties and Privacy Office (CLPO) used the Fair Information Practice Principles (FIPP)[1] as an initial tool to describe the existing civil liberties and privacy protections in place for collection done under Section 702 authority.[2]

SECTION 702 OF FISA

Section 702 of FISA was widely and publicly debated in Congress both during the initial passage in 2008 and the subsequent re-authorization in 2012. It provides a statutory basis for NSA, with the compelled assistance of electronic communication service providers, to target non-U.S. persons reasonably believed to be located outside the U.S. in order to acquire foreign intelligence information. Given that Section 702 only allows for the targeting of non-U.S. persons outside the U.S., it differs from most other sections of FISA. It does not require an individual determination by the U.S. Foreign Intelligence Surveillance Court (FISC) that there is probable cause to believe the target is a foreign power or an agent of a foreign power. Instead, the FISC reviews annual topical certifications executed by the Attorney General (AG) and the Director of National Intelligence (DNI) to determine if these certifications meet the statutory requirements. The FISC also determines whether the statutorily required targeting and minimization procedures used in connection with the certifications are consistent with the statute and the Fourth Amendment. The targeting procedures are designed to ensure that Section 702 is only used to target non-U.S. persons reasonably believed to be located outside the U.S.

The minimization procedures are designed to minimize the impact on the privacy on U.S. persons by minimizing the acquisition, retention, and dissemination of non-publicly available U.S. person information that was lawfully, but incidentally acquired under Section 702 by the targeting of non-U.S. persons reasonably believed to be located outside the U.S. Under these certifications the AG and the DNI issue directives to electronic communication service providers (service providers) that require these service providers to "immediately provide the Government with all information … or assistance necessary to accomplish the acquisition [of foreign intelligence information] in a manner that will protect the secrecy of the acquisition…." The Government's acquisition of communications under its Section 702 authority thus takes place pursuant to judicial review and with the knowledge of the service providers.

NSA cannot intentionally use Section 702 authority to target any U.S. citizen, any other U.S. person, or anyone known at the time of acquisition to be located within the U.S. The statute also prohibits the use of Section 702 to intentionally acquire any communication as to which the

[1] The FIPPS are the recognized principles for assessing privacy impacts. They have been incorporated into EO13636, *Improving Critical Infrastructure Cybersecurity* and the National Strategy for Trusted Identities in Cyberspace. These principles are rooted in the U.S. Department of Health, Education and Welfare's seminal 1973 report, "Records, Computers and the Rights of Citizens." The FIPPs have been implemented in the Privacy Act of 1974, with certain exemptions, including ones that apply to certain national security and law enforcement activities.

[2] NSA CLPO will continue to refine its assessment tools to best suit the mission of NSA, as a member of the Intelligence Community, and to protect civil liberties and privacy.

sender and all intended recipients are known at the time of acquisition to be located inside the U.S. Similarly, the statute prohibits the use of Section 702 to conduct "reverse targeting" (i.e., NSA may not intentionally target a person reasonably believed to be located outside of the U.S. if the purpose of such acquisition is to target a person reasonably believed to be located inside the U.S.). All acquisitions conducted pursuant to Section 702 must be conducted in a manner consistent with the Fourth Amendment. NSA's FISC-approved targeting procedures permit NSA to target a non-U.S. person reasonably believed to be located outside the U.S. if the intended target possesses, is expected to receive, and/or is likely to communicate foreign intelligence information concerning one of the certifications executed by the AG and DNI. Although the purpose of Section 702 is to authorize targeting of non-U.S. persons outside the U.S., the statute's requirement for minimization procedures recognizes that such targeted individuals or entities may communicate about U.S. persons or with U.S. persons. For this reason, NSA also must follow FISC-approved minimization procedures that govern the handling of any such communications.

NSA must report to the Office of the Director of National Intelligence (ODNI) and the Department of Justice (DOJ) any and all instances where it has failed to comply with the targeting and/or minimization procedures. In addition, ODNI and DOJ have access to documentation concerning each of NSA's Section 702 targeting decisions and conduct regular reviews in order to provide independent oversight of NSA's use of the authority. The FISC Rules of Procedure require the Government to notify the Court of all incidents of non-compliance with applicable law or with an authorization granted by the Court. The Government reports Section 702 compliance incidents to the Court via individual notices and quarterly reports. In addition, the Government reports all Section 702 compliance incidents to Congress in the Attorney General's Semiannual Report. Depending on the type or severity of compliance incident, NSA may also promptly notify the Congressional Intelligence Committees, as well as the President's Intelligence Oversight Board of an individual compliance matter.

Existing Privacy and Civil Liberties Protections: Each of the three branches of federal government oversees NSA's use of the Section 702 authorities. NSA provides transparency to its oversight bodies (Congress, DOJ, ODNI, DoD, the President's Intelligence Oversight Board and the FISC) through regular briefings, court filings, and incident reporting. In addition, DOJ and ODNI conduct periodic reviews of NSA's use of the authority and report on those reviews. More recently, at the direction of the President, the Government has provided additional transparency to the public regarding the program by declassifying FISC opinions and related documents. Although FISA surveillance is normally kept secret from the targets of the surveillance, there are exceptions. For example, if the Government intends to use the results of FISA surveillance, to include Section 702 surveillance, in a trial or other proceeding against a person whose communications were collected, the Government must notify the person so the person can challenge whether the communications were acquired lawfully. These protections implement the general Fair Information Practice Principle (FIPP) of transparency.

HOW NSA IMPLEMENTS SECTION 702 of FISA

TRAINING

Before an analyst gains access to any NSA signals intelligence data, the analyst must complete specialized training on the legal and policy guidelines that govern the handling and use of the data. Additional training is required for access to Section 702 data. These annual mandatory training requirements include scenario-based training, required reading, and a final competency test. The analyst must pass this test before being granted access. Furthermore, if a compliance incident involves a mistake or misunderstanding of relevant policies, the analyst is re-trained in order to continue to have access to the data acquired pursuant to Section 702.

IDENTIFYING AND TASKING A SELECTOR

Next in the Section 702 process is for an NSA analyst to identify a non-U.S. person located outside the U.S. who has and/or is likely to communicate foreign intelligence information as designated in a certification. For example, such a person might be an individual who belongs to a foreign terrorist organization or facilitates the activities of that organization's members. Non-U.S. persons are not targeted unless NSA has reason to believe that they have and/or are likely to communicate foreign intelligence information as designated in a certification; U.S. persons are never targeted.

Once the NSA analyst has identified a person of foreign intelligence interest who is an appropriate target under one of the FISC-approved Section 702 certifications, that person is considered the target. The NSA analyst attempts to determine how, when, with whom, and where the target communicates. Then the analyst identifies specific communications modes used by the target and obtains a unique identifier associated with the target – for example, a telephone number or an email address. This unique identifier is referred to as a selector. The selector is not a "keyword" or particular term (e.g., "nuclear" or "bomb"), but must be a specific communications identifier (e.g., e-mail address).

Next the NSA analyst must verify that there is a connection between the target and the selector and that the target is reasonably believed to be (a) a non-U.S. person and (b) located outside the U.S. This is not a 51% to 49% "foreignness" test. Rather the NSA analyst will check multiple sources and make a decision based on the totality of the information available. If the analyst discovers any information indicating the targeted person may be located in the U.S. or that the target may be a U.S. person, such information must be considered. In other words, if there is conflicting information about the location of the person or the status of the person as a non-U.S. person, that conflict must be resolved before targeting can occur.

For each selector, the NSA analyst must document the following information: (1) the foreign intelligence information expected to be acquired, as authorized by a certification, (2) the information that would lead a reasonable person to conclude the selector is associated with a

non-U.S. person, and (3) the information that would similarly lead a reasonable person to conclude that this non-U.S. person is located outside the U.S. This documentation must be reviewed and approved or denied by two senior NSA analysts who have satisfied additional training requirements. The senior NSA analysts may ask for more documentation or clarification, but regardless must verify that all requirements have been met in full. NSA tracks the submission, review, and approval process through the documentation and the senior NSA analysts' determinations are retained for further review by NSA's compliance elements, as well as external oversight reviewers from DOJ and ODNI. Upon approval, the selector may be used as the basis for compelling a service provider to forward communications associated with the given selector. This is generally referred to as "tasking" the selector.

Existing Privacy and Civil Liberties Protections: NSA trains its analysts extensively through a variety of means to ensure that analysts fully understand their responsibilities and the specific scope of this authority. If the analyst fails to meet the training standards, the analyst will not have the ability to use the Section 702 authority for collection purposes. If the analyst fails to maintain ongoing training standards, the analyst will lose the ability to use the Section 702 authority for collection purposes and all ability to retrieve any data previously collected under the authority. NSA requires any authorized and trained analyst seeking to task a selector using Section 702 to document the three requirements for use of the authority – that the target is connected sufficiently to the selector for an approved foreign intelligence purpose, that the target is a non-U.S. person, and that the target is reasonably believed to be located outside the U.S. This documentation must be reviewed, validated, and approved by the senior analysts who have received additional training. These protections implement the general FIPPs of purpose specification, accountability and auditing, and minimization.

ACCESSING AND ASSESSING COMMUNICATIONS OBTAINED UNDER SECTION 702 AUTHORITY

Once senior analysts have approved a selector as compliant, the service providers are legally compelled to assist the government by providing the relevant communications. Therefore, tasking under this authority takes place with the knowledge of the service providers. NSA receives information concerning a tasked selector through two different methods.

In the first, the Government provides selectors to service providers through the FBI. The service providers are compelled to provide NSA with communications to or from these selectors. This has been generally referred to as the PRISM program.

In the second, service providers are compelled to assist NSA in the lawful interception of electronic communications to, from, or about tasked selectors. This type of compelled service provider assistance has generally been referred to as Upstream collection. NSA's FISC-approved targeting procedures include additional requirements for such collection designed to prevent acquisitions of wholly domestic communications. For example, in certain circumstances NSA's procedures require that it employ an Internet Protocol filter to ensure that the target is

located overseas. The process for approving the selectors for tasking is the same for both PRISM and Upstream collection.

Once NSA has received communications of the tasked selector, NSA must follow additional FISC-approved procedures known as the minimization procedures. These procedures require NSA analysts to review at least a sample of communications acquired from all selectors tasked under Section 702, which occurs on a regular basis to verify that the reasonable belief determination used for tasking remains valid.

The NSA analyst must review a sample of communications received from the selectors to ensure that they are in fact associated with the foreign intelligence target and that the targeted individual or entity is not a U.S. person and is not currently located in the U.S. If the NSA analyst discovers that NSA is receiving communications that are not in fact associated with the intended target or that the user of a tasked selector is determined to be a U.S. person or is located in the U.S., the selector must be promptly "detasked." As a general rule, in the event that the target is a U.S. person or in the U.S., all other selectors associated with the target also must be detasked.

Existing Privacy and Civil Liberties Protections: In addition to extensive training, the analyst is required to review the collection to determine that it is associated with the targeted selector and is providing the expected foreign intelligence shortly after the tasking starts and at least annually thereafter. This review allows NSA to identify possible problems with the collection and provides an additional layer of accountability. In addition, NSA has technical measures that alert the NSA analysts if it appears a selector is being used from the U.S. These protections implement the general FIPPs of purpose specification, minimization, accountability and auditing, data quality, and security.

NSA PROCESSING AND ANALYSIS OF COMMUNICATIONS OBTAINED UNDER SECTION 702 AUTHORITY

Communications provided to NSA under Section 702 are processed and retained in multiple NSA systems and data repositories. One data repository, for example, might hold the contents of communications such as the texts of emails and recordings of conversations, while another, may only include metadata, i.e., basic information about the communication, such as the time and duration of a telephone call, or sending and receiving email addresses.

NSA analysts may access communications obtained under Section 702 authority for the purpose of identifying and reporting foreign intelligence. They access the information via "queries," which may be date-bound, and may include alphanumeric strings such as telephone numbers, email addresses, or terms that can be used individually or in combination with one another. FISC-approved minimization procedures govern any queries done on Section 702-derived information. NSA analysts with access to Section 702-derived information are trained in the proper construction of a query so that the query is reasonably likely to return valid foreign

intelligence and minimizes the likelihood of returning non-pertinent U.S. person information. Access by NSA analysts to each repository is controlled, monitored, and audited. There are, for example, automated checks to determine if an analyst has completed all required training prior to returning information responsive to a query. Further, periodic spot checks on queries by NSA analysts are conducted.

Since October 2011 and consistent with other agencies' Section 702 minimization procedures, NSA's Section 702 minimization procedures have permitted NSA personnel to use U.S. person identifiers to query Section 702 collection when such a query is reasonably likely to return foreign intelligence information. NSA distinguishes between queries of communications content and communications metadata. NSA analysts must provide justification and receive additional approval before a content query using a U.S. person identifier can occur. To date, NSA analysts have queried Section 702 content with U.S. person identifiers less frequently than Section 702 metadata. For example, NSA may seek to query a U.S. person identifier when there is an imminent threat to life, such as a hostage situation. NSA is required to maintain records of U.S. person queries and the records are available for review by both DOJ and ODNI as part of the external oversight process for this authority. Additionally, NSA's procedures prohibit NSA from querying Upstream data with U.S. person identifiers.

Existing Privacy and Civil Liberties Protections: In addition to the training and access controls, NSA maintains audit trails for all queries of the Section 702 data. NSA's Signals Intelligence Directorate's compliance staff routinely reviews a portion of all queries that include U.S. person identifiers to ensure that all such queries are only conducted when appropriate. Personnel from DOJ and ODNI provide an additional layer of oversight to ensure that NSA is querying the data appropriately. These protections implement the general FIPPs of security, accountability and auditing, and data quality.

NSA DISSEMINATION OF INTELLIGENCE DERIVED FROM COMMUNICATIONS OBTAINED UNDER SECTION 702 AUTHORITY

NSA only generates signals intelligence reports when the information meets a specific intelligence requirement, regardless of whether the proposed report contains U.S. person information. Dissemination of information about U.S. persons in any NSA foreign intelligence report is expressly prohibited unless that information is necessary to understand foreign intelligence information or assess its importance, contains evidence of a crime, or indicates a threat of death or serious bodily injury. Even if one or more of these conditions apply, NSA may include no more than the minimum amount of U.S. person information necessary to understand the foreign intelligence or to describe the crime or threat. For example, NSA typically "masks" the true identities of U.S. persons through use of such phrases as "a U.S. person" and the suppression of details that could lead to him or her being successfully identified by the context. Recipients of NSA reporting can request that NSA provide the true identity of a masked U.S. person referenced in an intelligence report if the recipient has a legitimate need to know the identity. Under NSA policy, NSA is allowed to unmask the identity only under certain

conditions and where specific additional controls are in place to preclude its further dissemination, and additional approval has been provided by one of seven designated positions at NSA. Additionally, together DOJ and ODNI review the vast majority of disseminations of information about U.S. persons obtained pursuant to Section 702 as part of their oversight process.

Existing Privacy and Civil Liberties Protections: As noted above, NSA only generates signals intelligence reports when the information meets a specific intelligence requirement, regardless of whether the proposed report contains U.S. person information or not. Additionally, NSA's Section 702 minimization procedures require any U.S. person information to be minimized prior to dissemination, thereby reducing the impact on privacy for U.S. persons. The information may only be unmasked in specific instances consistent with the minimization procedures and NSA policy. These protections implement the general FIPPs of minimization and purpose specification.

RETENTION OF UNEVALUATED COMMUNICATIONS OBTAINED UNDER SECTION 702 AUTHORITY

The maximum time that specific communications' content or metadata may be retained by NSA is established in the FISC-approved minimization procedures. The unevaluated content and metadata for PRISM or telephony data collected under Section 702 is retained for no more than five years. Upstream data collected from Internet activity is retained for no more than two years. NSA complies with these retention limits through an automated process.

NSA's procedures also specify several instances in which NSA must destroy U.S. person collection promptly upon recognition. In general, these include any instance where NSA analysts recognize that such collection is clearly not relevant to the authorized purpose of the acquisition nor includes evidence of a crime. Additionally, absent limited exceptions, NSA must destroy any communications acquired when any user of a tasked account is found to have been located in the U.S. at the time of acquisition.

Existing Privacy and Civil Liberties Protections: NSA has policies, technical controls, and staff in place to ensure the data is retained in accordance with the FISC-approved procedures. The automated process to delete the collection at the end of the retention period applies to both U.S. person and non U.S. person the information. There is an additional manual process for the destroying information related to U.S. Persons where NSA analysts have recognized the collection is clearly not relevant to the authorized purpose of the acquisition nor includes evidence of a crime. These protections implement the general FIPPs of minimization and security.

ORGANIZATIONAL MANAGEMENT, COMPLIANCE, AND OVERSIGHT

NSA is subject to rigorous internal compliance and external oversight. Like many other regulated entities, NSA has an enterprise-wide compliance program, led by NSA's Director of Compliance, a position required by statute. NSA's compliance program is designed to provide precision in NSA's activities to ensure that they are consistently conducted in accordance with law and procedure, including in this case the Section 702 certifications and accompanying Section 702 targeting and minimization procedures and additional FISC requirements. As part of the enterprise-wide compliance structure, NSA has compliance elements throughout its various organizations. NSA also seeks to detect incidents of non-compliance at the earliest point possible. When issues of non-compliance arise regarding the way in which NSA carries out the FISC-approved collection, NSA takes corrective action and, in parallel, NSA must report incidents of non-compliance to ODNI and DOJ for further reporting to the FISC and Congress, as appropriate or required.

These organizations, along with the NSA General Counsel, the NSA Inspector General, and most recently the Director of Civil Liberties and Privacy have critical roles in ensuring all NSA operations proceed in accordance with the laws, policies, and procedures governing intelligence activities. Additionally, each individual NSA analyst has a responsibility for ensuring that his or her personal activities are similarly compliant. Specifically, this responsibility includes recognizing and reporting all situations in which he or she may have exceeded his or her authority to obtain, analyze, or report intelligence information under Section 702 authority.

Compliance: NSA reports all incidents in which, for example, it has or may have inappropriately queried the Section 702 data, or in which an analyst may have made typographical errors or dissemination errors. NSA personnel are obligated to report when they believe NSA is not, or may not be, acting consistently with law, policy, or procedure. If NSA is not acting in accordance with law, policy, or procedure, NSA will report through its internal and external intelligence oversight channels, conduct reviews to understand the root cause, and make appropriate adjustments to its procedures.

If NSA discovers that it has tasked a selector that is used by a person in the U.S. or by a U.S. person, then NSA must cease collection immediately and, in most cases must also delete the relevant collected data and cancel or revise any disseminated reporting based on this data. NSA encourages self-reporting by its personnel and seeks to remedy any errors with additional training or other measures as necessary. Following an incident, a range of remedies may occur: admonishment, written explanation of the offense, request to acknowledge a training point that the analyst might have missed during training, and/or required retesting. In addition to reporting described above, any intentional violation of law would be referred to the NSA Office of Inspector General. To date there have been no such instances, as most recently confirmed by the President's Review Group on Intelligence and Communications Technology.

External Oversight: As required by the Section 702 targeting procedures, both DOJ and ODNI conduct routine oversight reviews. Representatives from both agencies visit NSA on a bi-monthly basis. They examine all tasking datasheets that NSA provides to DOJ and ODNI to determine whether the tasking sheets meet the documentation standards required by NSA's targeting procedures and provide sufficient information for the reviewers to ascertain the basis for NSA's foreignness determinations. For those records that satisfy the standards, no additional documentation is requested. For those records that warrant further review, NSA provides additional information to DOJ and ODNI during or following the onsite review. NSA receives feedback from the DOJ and ODNI team and incorporates this information into formal and informal training to analysts. DOJ and ODNI also review the vast majority of disseminated reporting that includes U.S. person information.

Existing Privacy and Civil Liberties Protections: The compliance and oversight processes allow NSA to identify any concerns or problems early in the process so as to minimize the impact on privacy and civil liberties. These protections implement the general FIPPs of transparency to oversight organizations and accountability and auditing.

CONCLUSION

This Report, prepared by NSA's Office of Civil Liberties and Privacy, provides a comprehensive description of NSA's Section 702 activities. The report also documents current privacy and civil liberties protections.

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

Plaintiff's Exhibit 25

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

An intrusion-detection system known as EINSTEIN 2.0 used to protect civilian unclassified networks in the Executive Branch against malicious network activity complies with the Fourth Amendment to the Constitution, the Wiretap Act, the Foreign Intelligence Surveillance Act, the Stored Communications Act, and the pen register and trap and trace provisions of chapter 206 of title 18, United States Code, provided that certain log-on banners or computer-user agreements are consistently adopted, implemented, and enforced by executive departments and agencies using the system.

January 9, 2009

MEMORANDUM OPINION FOR THE COUNSEL TO THE PRESIDENT

As part of the Comprehensive National Cybersecurity Initiative, the Department of Homeland Security ("DHS"), in coordination with the Office of Management and Budget, is in the process of establishing an intrusion-detection system known as EINSTEIN 2.0 in order to detect unauthorized network intrusions and data exploitations against the Executive Branch's civilian unclassified computer systems ("Federal Systems").[1] In January 2007, you asked this Office to undertake a legal review of proposed EINSTEIN 2.0 operations; since that time we have provided ongoing informal advice regarding the legality of those operations, which are now underway. This memorandum formalizes the informal advice we have provided regarding whether EINSTEIN 2.0 operations comply with the Fourth Amendment to the Constitution of the United States, title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 211, 18 U.S.C. § 2510 *et seq.* (2006), as amended ("the Wiretap Act"), the Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, 92 Stat. 1783, 50 U.S.C.A. § 1801 *et seq.* (West 2008), as amended ("FISA"), the Stored Communications Act, Pub. L. No. 99-508, Tit. II, 100 Stat. 1848 (1986), 18 U.S.C. § 2701 *et seq.* (2006), as amended ("SCA"), and the pen register and trap and trace provisions of title 18, United States Code, 18 U.S.C. § 3121 *et seq.* (2006), as amended ("Pen/Trap Act").

We examine these legal issues in the context of an executive department's or agency's use of a model computer log-on banner or a model computer-user agreement developed by lawyers from the Department of Justice ("DOJ"), DHS, and other departments and agencies with expertise in cybersecurity issues. We conclude that as long as executive departments and agencies participating in EINSTEIN 2.0 operations consistently adopt, implement, and enforce the model log-on banner or computer-user agreement—or log-on banners or computer-user agreements with terms that are substantially equivalent to those models—the use of EINSTEIN 2.0 technology to detect computer network intrusions and exploitations against Federal Systems complies with the Fourth Amendment, the Wiretap Act, FISA, the SCA, and the Pen/Trap Act.

[1] As used this memorandum, the term "Federal Systems" includes all Executive Branch federal Government information systems except for National Security Systems of executive departments and agencies and Department of Defense information systems.

I.

Over the past several years, Federal Systems have been subject to sophisticated and well-coordinated computer network intrusions and exploitations on an unprecedented scale. The Intelligence Community has determined that those malicious network activities pose a grave threat to national security. *See also* Center for Strategic and International Studies, *Securing Cyberspace* 11-15 (2008) (discussing national security implications of federal network vulnerabilities). Those malicious network activities occur at the hands of hostile foreign nations (including foreign intelligence services), transnational criminal groups and enterprises, and individual computer hackers. Recent intrusions and exploitations have resulted in the theft of significant amounts of unclassified data from many executive departments and agencies, as well as information regarding the vulnerabilities of Federal Systems. The unclassified networks of the Departments of Defense, State, Homeland Security, and Commerce, among others, have suffered intrusions against their networks and exploitations of their data. Accordingly, the Homeland Security Council has determined that the deployment of a multi-layered network defense system is necessary to protect Federal Systems against these ongoing computer intrusions and exploitations carried out by a broad array of cyber adversaries.

The first layer of this network-defense system is known as EINSTEIN 1.0 and already is in place across segments of several Executive Branch agencies. EINSTEIN 1.0 is a semi-automated process for detecting—albeit after the fact—inappropriate or unauthorized inbound and outbound network traffic between participating departments and agencies and the Internet. The United States Computer Emergency Readiness Team ("US-CERT"), an organizational component of DHS, administers EINSTEIN 1.0.

EINSTEIN 1.0 analyzes only "packet header" information—and not packet "payload" (content) information—for inbound and outbound Internet traffic of participating agencies.[2] The header information collected by EINSTEIN 1.0 technology includes: the source and destination IP addresses for the packet, the size of the data packet, the specific Internet protocol used (for e-mail, the Simple Mail Transfer Protocol and, for use of the World Wide Web, the Hypertext Transport Protocol), and the date and time of transmission of the packet (known as "the date/time stamp"). EINSTEIN 1.0 collects this information only after packets already have been sent or received by a user, and, thus, does not provide real-time information regarding network intrusions and exploitations against Federal Systems. US-CERT analysts examine the header information to identify suspicious inbound and outbound Internet traffic, particularly network backdoors and intrusions, network scanning activities, and computer network exploitations using viruses, worms, spyware, bots, Trojan horses, and other "malware."

[2] The Internet consists of millions of computers connected by a network of fiber-optic cables and other data-transmission facilities. Data transmitted across the Internet are broken down into "packets" that are sent out from one computer to another. Each packet is directed (routed) to its intended source from its respective destination by an Internet Protocol ("IP") address. An IP address is a unique numerical address, akin to a phone number or physical address, identifying each computer on the Internet. Each packet may follow a different route to its ultimate IP address destination, traveling over the networks of several different Internet backbone providers and Internet Service Providers ("ISPs") before arriving at the destination. Upon arrival at the destination, the packets are reconstituted. *See generally* Jonathan E. Nuechterlein & Philip J. Weiser, *Digital Crossroads* 121-28 (2005).

EINSTEIN 1.0 contains several limitations. First, it does not provide real-time reporting regarding intrusions and exploitations against Federal Systems. Second, it does not cover all Federal Systems, and, therefore, does not provide complete awareness regarding malicious network activity directed against those systems. Third, because EINSTEIN 1.0 does not scan packet content, it does not offer complete intrusion and exploitation detection functionality.

We understand that many executive departments and agencies supplement EINSTEIN 1.0 with their own intrusion-detection systems, which are designed to identify network intrusions and exploitations conducted against their own computer systems. In addition, individual departments and agencies also operate their own network filters to block certain unauthorized content, such as Internet pornography and file-sharing activities, among others. We understand, however, that there is little or no coordination or communication among Executive Branch entities conducting these individualized network defense activities. Accordingly, multiple departments facing the same intrusion or exploitation might have no idea that they are all facing a coordinated malicious network operation. Nor would departments or agencies that have not yet been subject to the intrusion or exploitation have advanced warning of the activity, such that they could upgrade their defenses. Hence, the lack of cybersecurity collaboration within the Executive Branch leads to inefficient network defensive measures that contribute to the ongoing vulnerability of Federal Systems.

To rectify this situation, DHS, in conjunction with OMB, is deploying throughout the Executive Branch an intrusion-detection system known as EINSTEIN 2.0 to provide greater coordination and situational awareness regarding malicious network activities directed against Federal Systems. EINSTEIN 2.0 is a robust system that is expected to overcome the technical limitations of EINSTEIN 1.0. EINSTEIN 2.0 technology is comprised of computers ("sensors") configured with commercial "off-the-shelf" intrusion-detection software as well as government-developed software. That technology will be located at certain Internet access points known as Trusted Internet Connections ("TICs"), which connect Federal Systems to the Internet.

EINSTEIN 2.0 intrusion-detection sensors will observe in near-real time the packet header and packet content of all incoming and outgoing Internet traffic of Federal Systems ("Federal Systems Internet Traffic") for the "signatures" of malicious computer code used to gain access to or to exploit Federal Systems.[3] *See generally* NIST Special Publication No. 800-94 (2007) (discussing signature-based detection techniques). Because Internet traffic is IP-address based, we understand that only Federal Systems Internet Traffic destined to or sent from an IP address associated with an executive department or agency participating in EINSTEIN 2.0 ("EINSTEIN 2.0 Participant") would be scanned by EINSTEIN 2.0 technology. Thus, EINSTEIN 2.0 technology will scan only the Federal Systems Internet Traffic for EINSTEIN 2.0 Participants that connect to the Internet at TICs.

DHS has the responsibility for determining which signatures to program into the EINSTEIN 2.0 sensors, pursuant to procedures developed by DHS. Signatures may be derived

[3] By the term "malicious computer code," we mean not only "malware," such as viruses, spyware, and Trojan horses, but also malicious network intrusion and exploitation activities, such as identifying network backdoors and network scanning activities, and so-called "social engineering" activities, such as "phishing" exploits that seek usernames, passwords, social security numbers, or other personal information.

from several sources, including commercial computer security services, publicly available computer security information, privately reported incidents to US-CERT, in-depth analysis by US-CERT analysts, and from other federal partners involved in computer defense. We understand that from information obtained through these sources, DHS will create signatures based upon known malicious computer code to guide the operations of EINSTEIN 2.0 sensors.

EINSTEIN 2.0 sensors will not scan actual Federal Systems Internet Traffic for malicious computer code as that traffic is in transmission, but instead will scan a temporary copy of that traffic created solely for the purpose of scanning by the sensors. The "original" Federal Systems Internet Traffic will continue to its destination without being scanned by EINSTEIN 2.0 sensors; thus, EINSTEIN 2.0 operations will not disrupt the normal operations of Federal Systems. But EINSTEIN 2.0 technology will create a temporary mirror image of all Federal Systems Internet Traffic of EINSTEIN 2.0 Participants for parallel scanning by the sensors. The temporary copy of Federal Systems Internet Traffic is created only for identifying known signatures. When EINSTEIN 2.0 sensors identify Federal Systems Internet Traffic containing packets with malicious computer code matching a signature, EINSTEIN 2.0 technology is designed to generate—in near-real time—an automated alert about the detected signature. The alert generally will not contain the content of the packet, but will include header information, such as the source or remote IP address associated with the traffic that generated the alert, metadata regarding the type of signature that was detected, and the date/time stamp.

In addition to generating automated alerts, EINSTEIN 2.0 operations will both acquire and store data packets from the mirror copy of Federal Systems Internet Traffic that are associated with a detected signature. Those packets, which may include the full content of Internet communications, such as e-mails, may be reviewed by analysts from US-CERT and other authorized persons involved in computer network defense. We understand that no packets other than those associated with a known signature will be acquired and stored. Accordingly, we understand that the vast majority of packets that are not associated with malicious computer code matching a signature will be deleted promptly. *See* Department of Homeland Security, *Privacy Impact Assessment for EINSTEIN 2*, at 12 (May 18, 2008) (stating that all "clean traffic" is promptly deleted).

We have been informed that EINSTEIN 2.0 operations are expected to improve substantially the Government's ability to defend Federal Systems against intrusions and exploitations. EINSTEIN 2.0 operations will supplement—and not replace—the current individualized computer network security defenses of executive departments and agencies with a centralized and coordinated network defense system operated by DHS. That centralization and coordination of information regarding all Federal Systems Internet Traffic is expected to facilitate real-time situational awareness regarding malicious network activity across all Federal Systems. Improved situational awareness in turn will facilitate improved defensive measures, such as minimizing network vulnerabilities and alerting users of Federal Systems about particular malicious computer code detected against particular EINSTEIN 2.0 Participants. By sharing information throughout the Executive Branch regarding signatures detected in Federal Systems Internet Traffic, EINSTEIN 2.0 operations should facilitate improved defenses against known malicious computer code.

As part of enrolling in EINSTEIN 2.0 operations, each EINSTEIN 2.0 Participant is required to enter into a memorandum of agreement ("MOA") with DHS. We understand that the MOA will require an EINSTEIN 2.0 Participant to certify that it has implemented procedures to provide appropriate notice to its employees that by using Government-owned information systems, the employee acknowledges and consents to the monitoring, interception, and search of his communications transiting through or stored on those systems, and that the employee has no reasonable expectation of privacy in his use of those systems.[4] Those procedures are to include computer-user agreements, log-on banners, and computer-training programs. We understand that DHS must receive that certification from each EINSTEIN 2.0 Participant before any of the Participant's Federal Systems Internet Traffic can be scanned by EINSTEIN 2.0 technology.

EINSTEIN 2.0 Participants will not be required to use a specific banner or user agreement. We have been advised that given the diversity of missions and organizations among departments and agencies within the Executive Branch and the varying technical constraints faced by those entities, there simply is no one-size-fits-all solution for providing notice to and obtaining the consent of employees for EINSTEIN 2.0 operations. We have been informed, however, that the MOA will include model log-on banner and model computer-user agreement language for EINSTEIN 2.0 Participants to consider in crafting their own banners and user agreements. The model language, which was developed by lawyers from DOJ with the input and advice of lawyers from DHS and other interested departments and agencies, is as follows:

- You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.

- Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

- By using this information system, you understand and consent to the following:

    - You have no reasonable expectation of privacy regarding communications or data transiting or stored on this information system.
    - At any time, and for any lawful government purpose, the Government may monitor, intercept, and search any communication or data transiting or stored on this information system.
    - Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.

[click button: I AGREE]

[4] Throughout this memorandum we refer to "Executive Branch employees" and to the "employees" of EINSTEIN 2.0 Participants. By using the word "employees," we do not mean to limit the requirement to provide appropriate notice and consent to only those persons in a common law employment relationship with the federal Government. Rather, the term "employees" in this memorandum should be understood to include "employees" as well as "officers," "contractors," and "agents" of EINSTEIN 2.0 Participants.

The model computer-user agreement language contains the same substantive terms as the model log-on banner, except that it requires a computer user to sign a document indicating that the user "understand[s] and consent[s]" to the foregoing terms. Although we understand that EINSTEIN 2.0 Participants will not be required to use the exact model log-on banner and model computer-user agreement language, each EINSTEIN 2.0 Participant must certify that its log-on banners, computer-user agreements, and other computer policies contain language that demonstrates consent is "clearly given" and "clearly obtained" before EINSTEIN 2.0 becomes operational for the Participant's Federal Systems Internet Traffic.[5]

DOJ has advised that with the consistent adoption, implementation, and enforcement of appropriate consent and notification procedures, EINSTEIN 2.0 operations would comply with the Fourth Amendment to the Constitution of the United States, the Wiretap Act, FISA, the SCA, and the Pen/Trap Act. The Department arrived at these conclusions after a lengthy review by the Office of the Deputy Attorney General, this Office, and, with respect to the statutes for which they have expertise, the National Security Division and the Computer Crimes and Intellectual Property Section of the Criminal Division. This memorandum explains the reasoning for those conclusions.

II.

We first explain the reasoning behind DOJ's conclusion that the deployment, testing, and use of EINSTEIN 2.0 technology complies with the Fourth Amendment where each EINSTEIN 2.0 Participant consistently adopts and implements the model log-on banner or model computer-user agreement—or a log-on banner or computer-user agreement containing substantially equivalent terms establishing that the consent of its employees is "clearly given" and "clearly obtained."

---

[5] For example, DOJ already has in place a log-on banner that we believe would satisfy the MOA's certification criteria. DOJ's banner at present provides:

- You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.
- Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.
- By using this information system, you understand and consent to the following:
  - You have no reasonable expectation of privacy regarding any communications transmitted through or data stored on this information system.
  - At any time, the Government may monitor, intercept, search and/or seize data transiting or stored on this information system.
  - Any communications transmitted through or data stored on this information system may be disclosed or used for any U.S. Government-authorized purpose.

[click button: I AGREE]

A.

The Fourth Amendment provides in relevant part: "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." U.S. Const. amend. IV. Government activity implicates the protections of the Fourth Amendment where it constitutes a "search" or a "seizure" within the meaning of the Fourth Amendment. The Supreme Court has said that a "search" occurs where the Government infringes upon a person's legitimate expectation of privacy, consisting of both an actual, subjective expectation of privacy as well as an objectively reasonable expectation of privacy—"*i.e.*, one that has a source outside the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society." *Minnesota v. Carter*, 525 U.S. 83, 88 (1998) (internal quotation marks omitted).

We think it plain that computer users exchanging Internet communications through Federal Systems lack a legitimate expectation of privacy in certain specific categories of data that will be subject to scanning by EINSTEIN 2.0 technology. There is no objectively reasonable expectation of privacy in information regarding the to/from addresses for e-mails, the IP addresses of Web sites visited, the total traffic volume of the user, and other addressing and routing information conveyed for the purpose of transmitting Internet communications to or from a user. *See Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 904-05 (9th Cir. 2008); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008); *see also Smith v. Maryland*, 442 U.S. 735, 743-44 (1979) (no legitimate expectation of privacy in dialing, routing, addressing, and signaling information transmitted to telephone companies). E-mail addresses and IP addresses provide addressing and routing information to an Internet Service Provider ("ISP") in the same manner as a telephone number provides switching information to a telephone company. *Forrester*, 512 F.3d at 510. Just as a telephone user has no objectively reasonable expectation of privacy in telephone numbers voluntarily turned over to the phone company to enable switching of a phone call, an Internet user has no such expectation of privacy in routing information submitted to an ISP in order to deliver an Internet communication. *Id.* That routing information also is akin to the addressing information written on the outside of a first-class letter, which also is not constitutionally protected. *Id.* at 511 ("E-mail, like physical mail, has an outside address 'visible' to the third-party carriers that transmit it to its intended location."). With respect to information regarding the total volume of data received and transmitted by an Internet user, that information is no different from the information produced by a pen register regarding the number of incoming and outgoing calls at a particular phone number; and the Supreme Court has long held that an individual has no legitimate expectation of privacy in such information, which already has been exposed to a telecommunications carrier for the purpose of routing a communication. *Id.* Therefore, because there is no legitimate expectation of privacy with respect to the foregoing information transmitted for the purpose of routing Internet communications, the scanning of that information by EINSTEIN 2.0 technology does not constitute a "search" subject to the restrictions of the Fourth Amendment.

With respect to a user's expectation of privacy in the content of an Internet communication (such as an e-mail), we assume for the purposes of this memorandum that a computer user generally has a legitimate expectation of privacy in that content while it is in

transmission over the Internet. To date, the federal courts appear to agree that the sender of an e-mail, like the sender of a letter via first-class mail, has an objectively reasonable expectation of privacy in the content of a message while it is in transmission. *See, e.g.*, *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) (analogizing expectation of e-mail user in privacy of e-mail to expectation of individuals communicating by regular mail); *United States v. Maxwell*, 45 M.J. 406, 418 (C.A.A.F. 1996) (sender of an e-mail generally "enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant"); *see also Quon*, 529 F.3d at 905 ("[U]sers do have a reasonable expectation of privacy in the content of their text messages vis-à-vis the service provider.").[6]

Here, EINSTEIN 2.0 technology will scan a mirror copy of the packet content of Federal Systems Internet Traffic—including packets that are part of e-mails—for malicious computer code associated with a signature while the e-mail is in transmission, and, thus, while a sender of the e-mail, we assume, generally retains an expectation of privacy in the content of that communication. Hence, the precise question for us is whether the Executive Branch's automatic scanning of Federal Systems Internet Traffic for malicious computer code would implicate a computer user's legitimate expectation of privacy in the content of his Internet communications. We consider the privacy expectations of two groups of computer users: (1) Executive Branch employees and (2) private individuals communicating with specific Executive Branch employees or with Executive Branch departments or agencies more generally.

1.

We first address the expectations of Executive Branch employees. The Supreme Court has rejected the contention that public employees "can never have a reasonable expectation of privacy in their place of work." *O'Connor v. Ortega*, 480 U.S. 709, 717 (1987) (plurality); *id.* at 729-31 (Scalia, J., concurring). "Individuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer." *Id.* at 717 (plurality). Nevertheless, there are reasons to doubt that an Executive Branch employee has a legitimate expectation of privacy in the content of his Internet communications made using Government-owned information systems. The text of the Fourth Amendment protects the right of the people to be secure only in "*their* persons, houses, papers, and effects." U.S. Const. amend. IV (emphasis added). Although an individual generally possesses a legitimate expectation of privacy in his own personal computer, *e.g.*, *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007); *Lifshitz*, 369 F.3d at 190, it is less clear that an Executive Branch employee has a

[6] It also appears that the federal courts agree that, again like the sender of a first-class letter, an individual has a "diminished" expectation of privacy in the content of an e-mail that "ha[s] already arrived at the recipient." *Lifshitz*, 369 F.3d at 190 (internal citations omitted); *see Guest v. Leis*, 225 F.3d 325, 333 (6th Cir. 2001) (individual does not have a reasonable expectation of privacy "in an e-mail that had already reached its recipient; at this moment, the e-mailer would be analogous to a letter-writer, whose expectation of privacy ordinarily terminates upon delivery of the letter"); *Maxwell*, 45 M.J. at 417 (once an e-mail, like a letter, "is received and opened, the destiny of the [e-mail] then lies in the control of the recipient . . . , not the sender"); *United States v. Jones*, No. 03-15131, 149 Fed. Appx. 954, 959 (11th Cir. Sept. 20, 2005) (unpublished) ("We have not addressed previously the existence of a legitimate expectation of privacy in text messages or e-mails. Those circuits that have addressed the question have compared e-mails with letters sent by postal mail. Although letters are protected by the Fourth Amendment, 'if a letter is sent to another, the sender's expectation of privacy ordinarily terminates upon delivery.'") (quoting *United States v. King*, 55 F.3d 1193, 1195-96 (6th Cir. 1995)).

legitimate expectation of privacy in Internet communications he makes using a computer that is the property of the United States Government, provided by the taxpayers for his use at work. *Cf. Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002) (Posner, J.) (employee "had no right of privacy in the computer that [his private employer] had lent him for use in the workplace"); *but cf. United States v. Slanina*, 283 F.3d 670, 677 (5th Cir. 2002) (employee had reasonable expectation of privacy in use of city-owned computer where there was no "city policy placing Slanina on notice that his computer usage would be monitored" and there was no "indication that other employees had routine access to his computer"), *vacated on other grounds*, 537 U.S. 802 (2002). A government employee lacks an ownership or other property interest in the computer he uses at work; and he especially lacks any such interests in the Federal Systems—the network infrastructure that the Government provides to enable its employees to access the Internet—that, unlike his personal computer, ordinarily is not within his day to day control.

As a general matter, however, the Supreme Court has held that there may be circumstances in which a government employee has a legitimate expectation of privacy in the contents of governmental property that the employee uses or controls at work, such as an office or a locked desk drawer. *See O'Connor*, 480 U.S. at 716-19 (1987) (plurality) (public employee has a reasonable expectation of privacy in personal items, papers, and effects in office, desk, and file cabinets provided by public employer); *see id.* at 730-31 (Scalia, J., concurring) (government employee has a legitimate expectation of privacy in the contents of his office). And the Court also has made it clear that property interests are not conclusive regarding the legitimacy of an individual's expectation of privacy. *See Oliver v. United States*, 466 U.S. 170, 183 (1984) ("The existence of a property right is but one element in determining whether expectations of privacy are legitimate."); *Warden v. Hayden*, 387 U.S. 294, 304 (1967) ("The premise that property interests control the right of the Government to search and seize has been discredited."); *see also Legality of Television Surveillance in Government Offices*, 3 Op. O.L.C. 64, 66-67 (1979) (government ownership of office insufficient to establish employee's lack of expectation of privacy where "in a practical sense" the employee exercises exclusive use of the office) ("*Television Surveillance Opinion*"); *but cf. United States v. Ziegler*, 474 F.3d 1184, 1191 (9th Cir. 2007) (private employee's "workplace computer . . . is quite different from the" property described in *O'Connor*, because the computer was owned by the company, was controlled jointly by the company and the employee, and was monitored to ensure that employees did not visit pornographic or other inappropriate Web sites).

Instead, whether, in a particular circumstance, a government employee has a legitimate expectation of privacy in his use of governmental property at work is determined by "[t]he operational realities of the workplace" and "by virtue of actual office practices and procedures, or by legitimate regulation." *O'Connor*, 480 U.S. at 717 (plurality); *see United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000) ("[O]ffice practices, procedures, or regulations may reduce legitimate privacy expectations."). Here, we believe that an Executive Branch employee will not have a legitimate expectation of privacy in the content of his Internet communications transmitted over Government-owned information systems, provided that EINSTEIN 2.0 Participants consistently adopt, implement, and enforce appropriate consent and notification procedures, such as the model log-on banner or model computer-user agreement.

Although the Supreme Court has not addressed the issue, the federal courts of appeals have held that the use of log-on banners or computer-user agreements, such as the models provided by DHS to EINSTEIN 2.0 Participants, can eliminate any legitimate expectation of privacy in the content of Internet communications made at work using Government-owned information systems. For example, in *United States v. Simons*, the computer-use policy at the Foreign Bureau of Information Services ("FBIS"), a division of the Central Intelligence Agency, expressly noted that FBIS would "'audit, inspect, and/or monitor'" employees' use of the Internet, "including all file transfers, all websites visited, and all e-mail messages, 'as deemed appropriate.'" 206 F.3d at 398 (quoting policy). The Fourth Circuit held that this policy "placed employees on notice that they could not reasonably expect that their Internet activity would be private" and that, "in light of the Internet policy, Simons lacked a legitimate expectation of privacy" in his use of the Internet at work. *Id.*

Likewise, in *United States v. Angevine*, 281 F.3d 1130 (10th Cir. 2002), the Tenth Circuit held that a professor at a state university had no reasonable expectation of privacy in his Internet use in light of a broadly worded computer-use policy and log-on banner. The computer-use policy stated that the university "'reserves the right to view or scan any file or software stored on the computer or passing through the network, and will do so periodically'" and has "'a right of access to the contents of stored computing information at any time for any purpose which it has a legitimate need to know.'" *Id.* at 1133 (quoting policy). The log-on banner provided that "'all electronic mail messages . . . contain no right of privacy or confidentiality except where Oklahoma or Federal statutes expressly provide for such status,'" and that the university may "'inspect electronic mail usage by any person at any time without prior notice as deemed necessary to protect business-related concerns . . . to the full extent not expressly prohibited by applicable statutes.'" *Id.* (quoting banner). The court held that these notices prevent university employees "from reasonably expecting privacy in data downloaded from the Internet onto [u]niversity computers," because users are warned that data "is not confidential either in transit or in storage" and that "network administrators and others were free to view data downloaded from the Internet." *Id.* at 1134.

The Eighth Circuit came to the same conclusion in *United States v. Thorn*, 375 F.3d 679 (8th Cir. 2004), *vacated on other grounds*, 543 U.S. 1112 (2005). In *Thorn*, a state employee had acknowledged in writing a computer-use policy, which warned that employees "'*do not* have any personal privacy rights regarding their use of [the agency's] information systems and technology. An employee's use of [the agency's] information systems and technology indicates that the employee understands and consents to [the agency's] right to inspect and audit all such use as described in this policy.'" *Id.* at 682 (quoting policy). As a result of this policy, the court held that the state employee "did not have any legitimate expectation of privacy with respect to the use and contents of his [work] computer," because under the agency's policy, employees have "no personal right of privacy with respect to their use of the agency's computers" and provides the state with a "right to access all of the agency's computers." *Id.* at 683.

The decisions of other federal courts that have addressed the issue support the proposition that actual and consistent use of log-on banners or computer-user agreements can eliminate any legitimate expectation of an employee in the privacy with respect to his Internet communications using Government-owned information systems. *See Biby v. Board of Regents*, 419 F.3d 845,

850-51 (8th Cir. 2005) (university computer policy warning user "not to expect privacy if the university has a legitimate reason to conduct a search" and that "computer files, including e-mail, can be searched" under certain conditions eliminates any reasonable expectation of privacy the use of the computer network); *Muick*, 280 F.3d at 743 (employer's announced policy of inspecting work computers "destroyed any reasonable expectation of privacy"); *United States v. Monroe*, 52 M.J. 326, 330 (C.A.A.F. 1999) (no reasonable expectation of privacy that network administrators would not review e-mail where banner stated that "users logging on to this system consent to monitoring"); *see also Heckenkamp*, 482 F.3d at 1147 ("[P]rivacy expectations may be reduced if the user is advised that information transmitted through the network is not confidential and that the systems administrators may monitor communications transmitted by the user.") (citing *Angevine*, 281 F.3d at 1134, and *Simons*, 206 F.3d at 398); *cf. Slanina*, 283 F.3d at 677 ("[G]iven the absence of a city policy placing Slanina on notice that his computer usage would be monitored and the lack of any indication that other employees had routine access to his computer, we hold that Slanina's expectation of privacy was reasonable."); *Leventhal v. Knapek*, 266 F.3d 64, 73-74 (2d Cir. 2001) (public employee had reasonable expectation of privacy in the contents of his office computer because his employer neither "had a general practice of routinely conducting searches of office computers" nor "had placed [him] on notice that he should have no expectation of privacy in the contents of his office computer").

In light of these decisions, we believe that an Executive Branch employee who has clicked through the model log-on banner or signed the model computer-user agreement—or a log-on banner or computer-user agreement containing substantially equivalent terms—would not have a legitimate expectation of privacy in the contents of Internet communications made using Government-owned information systems and transmitted over Federal Systems. The model log-on banner is explicit and comprehensive regarding an employee's lack of a legitimate expectation of privacy in his use of Government-owned information systems. That banner states that the information system the employee uses is the property of the Government and "is provided for U.S. Government-authorized use only." The user "understand[s] and consent[s]" that: he has "no reasonable expectation of privacy regarding communications or data transiting or stored" on that information system; "[a]t any time, and for any lawful government purpose, the Government may monitor, intercept, and search any communication or data transiting or stored" on the information system; and any communications transmitted through or data stored on the information system "may be disclosed or used for any lawful government purpose." *See supra* pp. 5-6. We believe that the current DOJ banner, which deviates from the model log-on banner and the model computer-user agreement language in some respects, is to the same effect. *See supra* n. 5. Both the model log-on banner and computer-user agreement and the current DOJ log-on banner are at least as robust as—and we think they are even stronger than—the materials that eliminated an employee's legitimate expectation of privacy in the content of Internet communications in *Simons*, *Angevine*, *Thorn*, *Biby*, and *Monroe*. Therefore, we believe that adoption of the language in those model materials by EINSTEIN 2.0 Participants would eliminate their employees' legitimate expectations of privacy in their uses of Government-owned information systems with respect to the lawful government purpose of protecting Federal Systems against network intrusions and exploitations.

It is important to note, however, that the use of log-on banners or computer-user agreements may not be sufficient to eliminate an employee's legitimate expectation of privacy if

the statements and actions of Executive Branch officials contradict these materials. Recently, in *Quon v. Arch Wireless Operating Company*, the Ninth Circuit held that a police officer had a legitimate expectation of privacy in the contents of text messages sent and received on his department-provided pager notwithstanding departmental policies, because informal guidance from the officer's superiors had established, in practice, that the department would not monitor the content of his text messages. *See* 529 F.3d at 906-07. Thus, the "operational reality" at the department established a reasonable expectation of privacy in the text messages sent through a department-provided pager. *Id.* at 907 (quoting *O'Connor*, 480 U.S. at 717). In light of *Quon*, management officials at EINSTEIN 2.0 Participants should be careful not to make statements—either formal or informal—or to adopt practices that contradict the clear position in a log-on banner or a computer-user agreement that an employee has no legitimate expectation of privacy in his use of Government-owned information systems.

2.

We next consider whether an individual in the private sector communicating with an Executive Branch employee (such as where an individual sends an e-mail to either the employee's governmental—i.e., work—or personal e-mail account) or with an EINSTEIN 2.0 Participant directly (such as where an individual browses the Web site of the participating department or agency) has a legitimate expectation of privacy in the content of those communications. We conclude that he does not, provided that EINSTEIN 2.0 Participants consistently adopt, implement, and enforce notice and consent procedures for Executive Branch employees, such as the model log-on banner or model computer-user agreement, or banners or user agreements with terms that are substantially equivalent to those models.

The Supreme Court has held repeatedly that "[t]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *United States v. Miller*, 425 U.S. 435, 443 (1976); *see SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) ("[W]hen a person communicates to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities."); *Smith*, 442 U.S. at 743-44 ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."). Accordingly, "[i]t is well[] settled" that where a person "reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information." *United States v. Jacobsen*, 466 U.S. 109, 117 (1984).

We believe this principle applies to a person e-mailing an Executive Branch employee at the employee's personal e-mail account, where the employee has agreed to permit the Government to monitor, intercept, and search all of his Internet communications and data transiting Government-owned information systems. By clicking through the model log-on banner or agreeing to the terms of the model computer-user agreement, an Executive Branch employee gives *ex ante* permission to the Government to intercept, monitor, and search "any communications" and "any data" transiting or stored on a Government-owned information

system for any "lawful purpose." That permission necessarily includes the interception, monitoring, and searching of all personal communications and data sent or received by an employee using that system for the purpose of protecting Federal Systems against malicious network activity.[7] Therefore, an individual who communicates with an employee who has agreed to permit the government to intercept, monitor, and search any personal use of the employee's Government-owned information systems has no Fourth Amendment right to prohibit the Government from doing what the employee has authorized. *See Jerry T. O'Brien, Inc.*, 467 U.S. at 743; *Jacobsen*, 466 U.S. at 117; *Miller*, 425 U.S. at 443.

This well-settled Fourth Amendment principle applies even where, for example, the sender of an e-mail to an employee's personal, Web-based e-mail account (such as Gmail or Hotmail) does not know of the recipient's status as a federal employee or does not anticipate that the employee might read an e-mail sent to a personal e-mail account at work. Indeed, it is well established that a person communicating with another (who turns out to be an agent for the government) assumes the risk that the person has agreed to permit the Government to monitor the contents of that communication. *See, e.g.*, *United States v. White*, 401 U.S. 745, 749-51 (1971) (plurality opinion) (no Fourth Amendment protection against government monitoring of communications through transmitter worn by undercover operative); *Hoffa v. United States*, 385 U.S. 293, 300-03 (1966) (information disclosed to individual who turns out to be a government informant is not protected by the Fourth Amendment); *Lopez v. United States*, 373 U.S. 427, 439 (1963) (same); *Rathbun v. United States*, 355 U.S. 107, 111 (1957) ("Each party to a telephone conversation takes the risk that the other party may have an extension telephone and may allow another to overhear the conversation. When such takes place there has been no violation of any privacy of which the parties may complain."); *United States v. Coven*, 662 F.2d 162, 173-74 (2d Cir. 1981) (individual has no expectation of privacy in documents given to or accessible by undercover informant). Therefore, where an employee agrees to let the Government intercept, monitor, and search any communication or data sent, received, or stored by a Government-owned information system, the Government's interception of the employee's Internet communications with individuals outside the Executive Branch does not infringe upon those individuals' legitimate expectations of privacy. *See also infra* pp. 16-21 (consent of employee).

We also think it clear that an individual submitting information directly to an EINSTEIN 2.0 Participant through the Internet—such as where an individual submits an application online or browses the public Web site of the Participant—has no legitimate expectation of privacy in

[7] The language of the model log-on banner and model computer-user agreement unambiguously applies to "any" communications and "any" data transiting through or stored on a Government-owned information system and clearly eliminates any reasonable expectation of privacy that a user could have with respect to such communications and data. Nevertheless, if a participating department or agency wished to add even more express notice that those terms apply to personal communications and personal data that an employee sends, receives, or stores using a Government-owned information system, such as the use of personal Web-based e-mail accounts at work, the department or agency could so in several ways. To be clear, we do not believe that any such efforts are legally required. But should a participating department or agency decide to go even further than the robust protection afforded by the model language, it would have several options at its disposal. For example, the department or agency could include in its log-on banner or computer-user agreement express language regarding personal communications or data. Or it could notify employees through computer training and certification programs that *any* personal use of Government-owned information systems by an employee is subject to interception, monitoring, and searching.

the contents of any information that he transmits to the department or agency. An individual has no expectation of privacy in communications he makes to a known representative of the Government. *See United States v. Caceres*, 440 U.S. 741, 750-51 (1979) (individual has no reasonable expectation of privacy in communications with IRS agent made in the course of an audit); *cf. Transmission by a Wireless Carrier of Information Regarding a Cellular Phone User's Physical Location to Public Safety Organizations*, 20 Op. O.L.C. 315, 321 (1996) (individual calling 911 lacks a reasonable expectation that information regarding his location will not be transmitted to public safety organizations) ("*Caller ID Opinion*"). Furthermore, an individual who communicates information to another individual who turns out to be an undercover agent of the Government has no legitimate expectation of privacy in the content of that information. *See supra* p. 13. *A fortiori*, where an individual is communicating with a *declared* agent of the Government—here, an executive department or agency—the individual does not have a legitimate expectation that his communication would not be monitored or acquired by the Government. It also is well established that an individual does not have any legitimate expectation of privacy in information that he reveals to a third party. *See supra* p. 12; *see also United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008) (individual has no legitimate expectation of privacy in computer files he made accessible to others); *United States v. King*, 509 F.3d 1338, 1342 (11th Cir. 2007) (individual has no legitimate expectation of privacy in computer files shared with others over network on military base). Hence, an individual could not possibly have a legitimate expectation of privacy in communications he shares directly with a department or agency of the Government. Indeed, the entire purpose of his online communication is for the Government to receive the content of his message. *Cf. Caller ID Opinion*, 20 Op. O.L.C. at 321 (purpose of calling 911 is to request governmental aid in an emergency). Therefore, we also do not believe that EINSTEIN 2.0 operations implicate a legitimate expectation of privacy in the content of Internet communications made between private individuals and an EINSTEIN 2.0 Participant.

B.

Even if EINSTEIN 2.0 operations were to constitute a "search" under the Fourth Amendment, we believe that those operations nonetheless would be consistent with that Amendment's "central requirement" that all searches be *reasonable*. *Illinois v. McArthur*, 531 U.S. 326, 330 (2001) (internal quotation marks omitted). Where, as here, the statutes and common law of the founding era do not provide a specific analogue, we analyze the reasonableness of a search in light of traditional judicial standards, balancing the degree of intrusion upon an individual's privacy in light of the search's promotion of legitimate governmental interests. *Virginia v. Moore*, 128 S. Ct. 1598, 1602-04 (2008). In many circumstances, a search is unreasonable unless law enforcement officials first obtain a warrant "issued by a neutral magistrate after finding probable cause." *McArthur*, 531 U.S. at 330. Yet the Supreme Court also has "made it clear that there are exceptions to the warrant requirement," *id.*, and that "neither a warrant nor probable cause, nor, indeed, any measure of individualized suspicion, is an indispensable component of reasonableness in every circumstance," *National Treasury Employees Union v. Von Raab*, 489 U.S. 656, 665 (1989).

One well-known exception to the need to obtain a warrant based upon probable cause is where a person consents to the search. *See Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973)

(consent is "one of the specifically established exceptions to the requirements of both a warrant and probable cause"). An Executive Branch employee who clicks "I agree" in response to the model log-on banner, enabling him to use Government-owned information systems to access the Internet, or an employee who signs the model computer-user agreement, thereby acknowledging his "consent[]" to monitoring of his use of those systems, certainly appears to have consented expressly to the scanning of his incoming and outgoing Internet communications.

In the context of public employment, however, merely obtaining the consent of an employee to search is not necessarily coextensive with the requirements of the Fourth Amendment. Such consent must be voluntary and cannot be obtained through duress or coercion. *See generally Schneckloth*, 412 U.S. at 223-35. Where an employee is confronted with the choice of either consenting to a search or facing adverse employment consequences, it is debatable whether consent is in fact voluntary. An Executive Branch employee who refuses to accept a log-on banner or to sign a computer-user agreement likely will not be able to access his computer and, hence, may be unable to perform his duties. *See, e.g.*, *Anobile v. Pelligrino*, 303 F.3d 107, 124 (2d Cir. 2002) ("[C]oercion may be found where one is given a choice between one's employment and one's constitutional rights.").

Indeed, putting a public employee to the choice of either consenting to an *unreasonable* search or facing potential adverse employment consequences may impose an invalid condition on public employment. Into the first part of the 20th Century, the Government "enjoyed plenary authority to condition public employment on the employee's acceptance of almost any term of employment including terms that restricted constitutional rights." Memorandum for the Attorney General, from Charles J. Cooper, Assistant Attorney General, Office of Legal Counsel, *Re: The Legality of Drug Testing Programs for Federal Employees* at 4 (Aug. 25, 1986) ("*Drug Testing Opinion*"). That view has since given way to the doctrine of unconstitutional conditions, which, as applied to public employment, prohibits the Government from conditioning employment on the relinquishment of a constitutional right, such as the First Amendment right to freedom of speech. *See, e.g.*, *Pickering v. Board of Educ.*, 391 U.S. 563, 568 (1968) ("'The theory that public employment, which may be denied altogether may be subjected to any conditions, regardless of how unreasonable, has been uniformly rejected.'") (quoting *Keyishian v. Board of Regents*, 385 U.S. 589, 605-06 (1967)). More than 20 years ago, we noted that the federal courts of appeals "have generally applied the doctrine of unconstitutional conditions" to conditions of employment that would require government employees to forgo their Fourth Amendment rights against unreasonable searches. *Drug Testing Opinion* at 7 ("[T]here appears to be a consensus that the doctrine of unconstitutional conditions applies in the Fourth Amendment context."). That statement is just as true today. *See, e.g.*, *Anobile*, 303 F.3d at 123-25 (search of dormitories of horse-racing industry employees' pursuant to their written consent unreasonable under the Fourth Amendment); *McGann v. Northeast Ill. Reg'l Commuter R.R. Corp.*, 8 F.3d 1174, 1180 (7th Cir. 1993) ("[T]he conditioning of access on the surrender of one's Fourth Amendment rights raises the specter of an unconstitutional condition."); *McDonell v. Hunter*, 807 F.2d 1302, 1310 (8th Cir. 1987) ("If a search is unreasonable, a government employer cannot require that its employees consent to that search as a condition of employment."); *Doyon v. Home Depot U.S.A., Inc.*, 850 F. Supp. 125, 129 (D. Conn. 1994) (Cabranes, J.) ("[C]onsent to an unreasonable search is not voluntary when required as a condition of employment.").

We do not believe, however, that the unconstitutional conditions doctrine applies here, because obtaining the consent of employees for EINSTEIN 2.0 operations does not require Executive Branch employees to consent to an *unreasonable* search. Notwithstanding that the terms of both the model log-on banner and the model computer-user agreement would permit monitoring of an employee's computer use for purposes other than network defense, we believe that the specific EINSTEIN 2.0 operations to which Executive Branch employees would be asked to consent would be reasonable.[8] Where, as here, an Executive Branch employee is being asked to consent only to a reasonable search, there is no invalid conditioning of public employment on the employee's relinquishment of his Fourth Amendment rights against unreasonable searches and no coercion that renders a search involuntary. *See, e.g.*, *United States v. Sihler*, 562 F.2d 349 (5th Cir. 1977) (prison employee's consent to routine search of his lunch bag valid); *cf. Drug Testing Opinion* at 7 ("[C]onsent to an *unreasonable* search is invalid.") (emphasis added); *Anobile*, 303 F.3d at 124 (similar); *McDonnell*, 807 F.2d at 1310 (similar). Thus, the inquiry regarding the voluntariness of an Executive Branch employee's consent merges with the underlying inquiry regarding the overall reasonableness of EINSTEIN 2.0 operations.[9] *See Drug Testing Opinion* at 7 ("[I]t appears that the government could not insist upon a complete waiver of Fourth Amendment rights as a condition of public employment and that the courts will scrutinize the search under the Fourth Amendment to determine whether it is reasonable.").

Therefore, we turn to the reasonableness of EINSTEIN 2.0 operations. A work-related administrative search by a public employer conducted for a non-law enforcement purpose is not *per se* unreasonable under the Fourth Amendment simply because the Government has not obtained a warrant based upon probable cause. The Supreme Court has said that "special needs, beyond the normal need for law enforcement," may render the warrant and probable cause provisions of the Fourth Amendment "impracticable for legitimate work-related, non-investigatory intrusions as well as investigations of work-related misconduct." *O'Connor*, 480 U.S. at 725 (plurality) (internal quotation marks and citations omitted); *id.* at 732 (Scalia, J., concurring) (searches in the government-employment context present "special needs"); *see also National Treasury Employees Union*, 489 U.S. at 665-66 (warrant and probable cause provisions of the Fourth Amendment are inapplicable to a search that "serves special governmental needs, beyond the normal need for law enforcement"); *Griffin v. Wisconsin*, 483 U.S. 868, 872 (1987) (special needs doctrine applies in circumstances that make the "warrant and probable cause requirement impracticable"). Rather, "public employer intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes

[8] Because the question presented to us is whether an employee's consent to conduct the particular scanning activities performed by EINSTEIN 2.0 technology would be valid under the Fourth Amendment, we do not address whether there would be valid consent to conduct any other search that could be conducted pursuant to the terms of the model log-on banner or the model computer-user agreement. *See Warshak v. United States*, 532 F.3d 521, 529-31 (6th Cir. 2008) (en banc) (rejecting premature Fourth Amendment challenge to facial constitutionality of provisions of the Stored Communications Act).

[9] Indeed, the consent of an employee is one factor the courts consider in determining whether a search by a public employer is reasonable. *See, e.g.*, *National Treasury Employees Union*, 489 U.S. at 672 & n.2 (considering consent to drug testing by Customs officers as one factor in concluding that such testing was reasonable); *United States v. Scott*, 450 F.3d 863, 868 (9th Cir. 2006) ("[S]earches of government employees still must be reasonable. . . . The employee's assent is merely a relevant factor in determining how strong his expectation of privacy is, and thus may contribute to a finding of reasonableness.") (internal citations omitted).

. . . should be judged by the standard of reasonableness under all the circumstances." *O'Connor*, 480 U.S. at 726 (plurality); *see id.* at 732 (Scalia, J., concurring).

Here, the Government plainly has a lawful, work-related, noninvestigatory purpose for the use of EINSTEIN 2.0's intrusion-detection system, namely the protection of Federal Systems against unauthorized network intrusions and exploitations. *See Heckenkamp*, 482 F.3d at 1148 (preventing misuse of and damage to university computer network is a lawful purpose); *see also National Treasury Employees Union*, 489 U.S. at 668 (special needs include government's need to "discover . . . latent or hidden" hazards); Federal Information Security Management Act of 2002, Public Law No. 107-347, § 301, 44 U.S.C. §§ 3541-3549 (2006) ("FISMA") (establishing purposes and authorities for the protection of federal information systems). As we have already noted, *see supra* p. 2, there is a substantial history of intrusions and exploitations against Federal Systems. The deployment of EINSTEIN 2.0 technology is designed to provide greater awareness regarding intrusions and exploitations against those Systems in order to facilitate improved network defenses against malicious network activity. Those goals are unrelated to the needs of ordinary criminal law enforcement. *See Heckenkamp*, 482 F.3d at 1147-48 (state university has "separate security interests" in maintaining integrity and security of its network that are unrelated to interest in law enforcement); *see also Illinois v. Lidster*, 540 U.S. 419, 424 (2004) (although ordinary law enforcement objectives do not qualify as "special needs," certain distinct "special law enforcement concerns" do); *Michigan Dep't of State Police v. Sitz*, 496 U.S. 444 (1990) (upholding highway checkpoint stops designed to detect and prevent drunk driving). It is true that DHS may share alerts of detected signatures associated with malicious computer code with other executive departments and agencies, including law enforcement agencies, as permitted by applicable law and DHS procedures. The disclosure of alert information to law enforcement agencies, however, is at most an ancillary, rather than a central, feature of EINSTEIN 2.0 operations. *Cf. Ferguson v. City of Charleston*, 532 U.S. 67, 79-80 (2001) ("central and indispensable feature" of hospital policy to screen obstetrics patients for cocaine was to facilitate "the use of law enforcement" tools—arrest and prosecution—"to coerce the patients into substance abuse treatment"); *City of Indianapolis v. Edmond*, 531 U.S. 32, 44 (2001) ("primary purpose" of narcotics checkpoints is to advance the "general interest" in "ordinary crime control"). We understand that EINSTEIN 2.0 operations are for the purpose of protecting Federal Systems, *see supra* pp. 4-5, and are not conducted in order to advance ordinary law enforcement goals. Therefore, we conclude that EINSTEIN 2.0 operations would advance special governmental needs distinct from the ordinary interest in criminal law enforcement.

Furthermore, it would be impracticable to require the Government to obtain a warrant based upon probable cause before deploying EINSTEIN 2.0 technology to detect malicious cyber activity against Federal Systems. The need for coordinated situational awareness regarding all intrusions and exploitations against Federal Systems is inconsistent with the requirement to obtain a warrant based upon probable cause. *See Board of Educ. v. Earls*, 536 U.S. 822, 828 (2002) (warrant and probable cause requirements are "peculiarly related to criminal investigations and may be unsuited to determining the reasonableness of administrative searches where the Government seeks to prevent the development of hazardous conditions"). Indeed, the goal of near-real time awareness of malicious network activity is incompatible with a requirement to obtain a warrant. Given the constant stream of intrusions and exploitations

against Federal Systems and the time it would take to seek and obtain a warrant, it would be entirely impracticable—if not impossible—to identify data packets containing malicious code in near real-time if the Government was required first to obtain a warrant before each such action. *See Skinner*, 489 U.S. at 623 (interest in dispensing with warrant requirement is at its strongest where "the burden of obtaining a warrant is likely to frustrate the governmental purpose behind the search") (internal quotation marks omitted). Requiring a particularized warrant based upon probable cause before a scan for each signature would introduce an element of delay, thus frustrating the Government's ability to collect information regarding intrusions and exploitations in a timely manner. *See Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995) (obtaining a warrant based upon probable cause is not a necessary element of reasonableness where such a requirement "would unduly interfere with the swift and informal" procedures needed to facilitate the government's special needs) (internal quotation marks omitted). Moreover, in light of the speed and frequency with which intrusion and exploitation techniques change, requiring the Government to obtain a warrant to use EINSTEIN 2.0 sensors to protect Federal Systems would require nearly continuous, ongoing, daily supervision by the courts of the details of the Government's network-defense activities. Such supervision would frustrate efforts to protect Federal Systems and to obtain new information regarding advanced intrusion and exploitation techniques. *See Heckenkamp*, 482 F.3d at 1148 ("[R]equiring a warrant to investigate potential misuse of the university's computer network would disrupt the operation of the university and the network that it relies upon in order to function."). For these reasons, we do not believe that EINSTEIN 2.0 operations would be presumptively unreasonable absent a warrant justified by probable cause.

Therefore, the reasonableness of EINSTEIN 2.0 operations is measured in light of the "totality of the circumstances," *United States v. Knights*, 534 U.S. 112, 118 (2001), in "the context within which a search takes place," *New Jersey v. T.L.O.*, 469 U.S. 325, 337 (1985). In the context of a workplace search by a public employer, the reasonableness analysis requires balancing the "invasion of the employees' legitimate expectation of privacy against the government's need for supervision, control, and the efficient operation of the workplace." *O'Connor*, 480 U.S. at 719-20 (plurality); *see Knights*, 534 U.S. at 118-19 (reasonableness inquiry balances, "on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which a search is needed for the promotion of legitimate governmental interests") (internal quotation marks omitted). A reasonable workplace search must be "justified at its inception" and "reasonably related in scope to the circumstances which justified the interference in the first place." *O'Connor*, 480 U.S. at 726 (plurality) (internal quotation marks omitted).

Based upon the information available to us, we believe that EINSTEIN 2.0 operations are reasonable under the totality of the circumstances. In light of the substantial history of intrusions and exploitations against Federal Systems, *see supra* p. 2, the deployment and use of EINSTEIN 2.0 technology to scan Federal Systems Internet Traffic of EINSTEIN 2.0 Participants for malicious computer code certainly is "justified at its inception." *O'Connor*, 480 U.S. at 726 (plurality) (internal quotation marks omitted).

We also conclude that any search conducted under EINSTEIN 2.0 operations would have a minimal impact upon the legitimate privacy expectations of computer users. The Supreme

Court has said that "[w]hen faced with . . . diminished expectations of privacy, minimal intrusions, or the like, certain general, or individual, circumstances may render a warrantless search or seizure reasonable." *McArthur*, 531 U.S. at 330. We already have noted that individuals have no legitimate expectation of privacy whatsoever in certain categories of information collected by EINSTEIN 2.0—e.g., to/from addresses for e-mails, the IP addresses of Web sites visited, and the total traffic volume of a user—generated in connection with the routing of Internet communications. *See supra* pp. 7-8. And in light of the notice and consent procedures that EINSTEIN 2.0 Participants must adopt under the MOA, we believe that an individual's expectation of privacy in the content of Internet communications transiting Federal Systems would, at a minimum, be significantly diminished. *See supra* pp. 10-14. Furthermore, we think it is reasonably likely that most Executive Branch employees and United States persons interacting with EINSTEIN 2.0 Participants and their employees neither intend to include nor want to receive malicious computer code in their e-mails and other Internet communications. And those who do intentionally unleash malicious computer code upon the Internet in order to conduct an unauthorized exploitation against Federal Systems have "no reasonable expectation of privacy" in the contents of those unauthorized Internet communications. 18 U.S.C. § 2510(21)(A).

We also conclude that the use of EINSTEIN 2.0 technology to detect malicious computer code in Federal Systems Internet Traffic imposes, at worst, a minimal burden upon legitimate privacy rights. Indeed, we understand that the actual scope of content monitoring by EINSTEIN 2.0 technology will be quite narrow. EINSTEIN 2.0 technology scans a mirror copy of the Federal Systems Internet Traffic of EINSTEIN 2.0 Participants. Of course, the EINSTEIN 2.0 technology will scan a copy of every single data packet of the Federal Systems Internet Traffic of those Participants. But we understand that the technology will scan that traffic—and only that traffic—only for particular malicious computer code associated with specific signatures. There is no authorization to acquire the content of any communication unrelated to detecting malicious computer code present in the packet. Therefore, we believe the intrusion upon any expectation of privacy in the privacy of the content of Internet communications that computer users may have vis-à-vis EINSTEIN 2.0 operations would be minimal, encompassing only the intrusion of searching for specified malicious computer code.

Our conclusion finds some support in the Supreme Court's cases holding that a search technique that reveals only unlawful activity is not subject to the Fourth Amendment at all. *See Jacobsen*, 466 U.S. at 123-24 (chemical field test that could disclose only whether white powder was cocaine does not infringe upon a legitimate expectation of privacy); *see also United States v. Place*, 462 U.S. 696, 706-07 (1983) (canine sniff by a well-trained narcotics detection dog that discloses only the present or absence of narcotics is "*sui generis*" because it "is so limited both in the manner in which the information is obtained and in the content of the information revealed by the procedure" and, therefore, does not intrude upon a legitimate expectation of privacy). The inclusion of malicious computer code in an e-mail or other Internet-based communication may or may not be analogous to the possession of contraband, such as narcotics, at issue in *Jacobsen* and *Place*. But the use of malicious computer code to gain access to Federal Systems is a federal offense, *see, e.g.*, 18 U.S.C. § 1030(a)(2)(B), (3), & (5)(A) (2006), and the inclusion of that code in, for example, an e-mail is far from "perfectly lawful activity," *Illinois v. Caballes*, 543 U.S.

405, 409-10 (2005) (emphasizing that a canine sniff detects only unlawful activity and does not implicate legitimate privacy interests).

We also find support in the decisions of federal appellate courts concluding that the use of a magnetometer (a metal detector) to scan for weapons at airports, courthouses, and other special locations is a reasonable search. *See, e.g.*, *United States v. Albardo*, 495 F.2d 799, 803-06 (2d Cir. 1974) (airport); *United States v. Epperson*, 454 F.2d 769, 771-72 (4th Cir. 1972) (airport); *Klarfield v. United States*, 944 F.2d 583, 586 (9th Cir. 1991) (courthouse). In those contexts, the Government's interests are compelling, and the magnetometer's ability to detect not only weapons, but also keys, belt buckles, jewelry, and other harmless items does not otherwise render its use an unreasonable search. *See United States v. Bell*, 464 F.2d 667, 675 (2d Cir. 1972) (Friendly, J.); *Epperson*, 454 F.2d at 771-72. Regardless whether the Government's interests here are on par with preventing hijacking or airport and courthouse violence, EINSTEIN 2.0 technology promotes the Government's network-defense interests through a more limited and precise intrusion. The information provided to us indicates that EINSTEIN 2.0 technology is more precisely calibrated than a magnetometer to detect the materials (here, malicious computer codes) that pose a threat. *See supra* pp. 3-4. Hence, we believe that, like the use of the magnetometer in certain contexts, the use of EINSTEIN 2.0 technology to detect malicious computer code in Federal Systems Internet Traffic is a reasonable activity.

Furthermore, we understand that any information acquired or shared by DHS in the course of EINSTEIN 2.0 operations shall be subject to minimization procedures that are designed to minimize the acquisition, retention, and dissemination of non-publicly available information concerning United States persons. So, for example, even to the extent EINSTEIN 2.0 operations would acquire the content of malicious computer code that overlaps with human-readable text—e.g., the "I love you" virus from several years ago, or social engineering techniques that rely upon regular e-mail text to encourage the recipient to submit sensitive information, including personally identifiable information—we understand that these minimization procedures are intended to reduce further the impact of EINSTEIN 2.0 operations upon the privacy interests of United States persons in the content of their Internet communications. *Cf. In re Sealed Case*, 310 F.3d 717, 740 (FISA Ct. Rev. 2002) (noting importance of minimization procedures in holding that electronic surveillance pursuant to FISA was reasonable under the Fourth Amendment). In addition, we understand that DHS is required to develop auditing, oversight, and training procedures to ensure that its employees follow the procedures developed with respect to minimizing and protecting United States person information. We further understand that DHS is required to develop procedures for the development of signatures to be programmed into the EINSTEIN 2.0 sensors, to ensure that the sensors are limited only to the detection of malicious computer code. In light of these safeguards, we believe that EINSTEIN 2.0 operations will have a minimal impact upon the legitimate privacy rights of computer users.

We conclude that the important governmental interest in protecting Federal Systems from intrusion and exploitation at the hands of foreign intelligence services, transnational criminal enterprises, and rogue computer hackers, *see supra* p. 2, outweighs the limited impact on the privacy rights, if any, of computer users communicating through Federal Systems. *See Heckenkamp*, 482 F.3d at 1148 (there is a "compelling government interest" in maintaining "the

security of its network" and in determining the source of "unauthorized intrusion into sensitive files"); *Vernonia Sch.*, 515 U.S. at 661 (government must identify "an interest that appears *important enough* to justify the particular search at hand"). Based upon the information provided to us, we believe that EINSTEIN 2.0 operations would constitute a "reasonably effective means" of promoting those interests. *Earls*, 536 U.S. at 837 (activity must be "a reasonably effective means of addressing" government's interest); *see Vernonia Sch.*, 515 U.S. at 663 (considering "the efficacy of [the] means for addressing the problem"). As explained *supra* pp. 4-5, EINSTEIN 2.0 operations are expected to improve the Government's situational awareness regarding computer network intrusions and exploitations against Federal Systems and to strengthen the ability to defend Federal Systems across the entire Executive Branch. Because EINSTEIN 2.0 technology is designed to detect and to store only malicious computer code associated with previously signatures, they also "are reasonably related in scope" to the problem EINSTEIN 2.0 is intended to address—the use of known malicious computer code to conduct intrusions and exploitations against Federal Systems. *O'Connor*, 480 U.S. at 726 (plurality) (internal quotation marks omitted).

Therefore, even if EINSTEIN 2.0 operations did involve a "search" within the meaning of the Fourth Amendment, we conclude that those operations nonetheless would satisfy the reasonableness requirement of the Fourth Amendment. For that same reason, we also conclude that an Executive Branch employee's agreement to the terms of the model log-on banner or the model computer-user agreement, or those of a banner or user agreement that are substantially equivalent to those models, constitutes valid, voluntary consent to the reasonable scope of EINSTEIN 2.0 operations, and, thus, does not impose any coercive unconstitutional condition upon federal employment.

III.

We now turn to the statutory issues. DOJ has advised that the deployment, testing, and use of EINSTEIN 2.0 technology would comply with the requirements of the Wiretap Act, FISA, the SCA, and the Pen/Trap Act where EINSTEIN 2.0 Participants obtain the consent of their employees through appropriate log-on banners or computer-user agreements. As we concluded with respect to the Fourth Amendment, we also conclude that EINSTEIN 2.0 operations would be consistent with the requirements of these statutes, provided that each EINSTEIN 2.0 Participant consistently adopts, implements, and enforces the model log-on banner or model computer-user agreement—or a log-on banner or computer-user agreement containing substantially equivalent terms establishing that the consent of its employees is "clearly given" and "clearly obtained."

A.

We begin with the Wiretap Act. The Wiretap Act, as amended by title I of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) ("ECPA"), and other subsequent statutes, prohibits the intentional "intercept[]" of any "electronic communication" unless authorized by law. 18 U.S.C. § 2511(1)(a) (2006); *see also id.* § 2511(1)(c) & (d) (prohibiting the intentional disclosure or use of the contents of electronic communications acquired in violation of section 2511(1)(a)). As relevant here, the Act defines

"intercept" as the "acquisition of the contents of any . . . electronic . . . communication through the use of any electronic, mechanical, or other device." *Id.* § 2510(4). EINSTEIN 2.0 technology would constitute a covered "device." *See id.* § 2510(5) (defining "electronic, mechanical, or other devices" as any device "which can be used to intercept a[n] . . . electronic communication other than" certain specified devices not applicable here).

Because use of the EINSTEIN 2.0 sensors requires the creation of a full mirror copy of the Federal Systems Internet Traffic of EINSTEIN 2.0 Participants, we conclude that the operation of those sensors "acqui[res] the contents" of an electronic communication within the meaning of the Act. The Wiretap Act defines "contents" to mean "any information concerning the substance, purport, or meaning" of a communication. 18 U.S.C. § 2510(8). And "electronic communication" is defined to mean "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, . . . electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce," with certain exceptions not applicable here. *Id.* § 2510(12). The courts have held that communications that have not been recorded (to a medium such as a computer disk), viewed, or listened to have not been "acquired" within the meaning of the Wiretap Act. *See, e.g.*, *United States v. Lewis*, 406 F.3d 11, 17-18 (1st Cir. 2004). Although the full mirror copy of Federal Systems Internet Traffic is only temporary, we believe the creation of the copy is sufficient to constitute an acquisition of the contents of communication under the Wiretap Act. Furthermore, even if creation of the temporary mirror copy were not sufficient to implicate the provisions of that Act, EINSTEIN 2.0 technology also acquires and stores, for later review by analysts, data packets from Federal Systems Internet Traffic containing malicious computer code associated with a signature. The acquisition and storage of these data packets, which are part of the "contents" of electronic communications, certainly constitutes an "intercept" within the meaning of the Wiretap Act. *See* 18 U.S.C. § 2510(4), (5), (8), & (12). Therefore, absent an exception, section 2511(1)(a) applies to at least some aspects of EINSTEIN 2.0 operations.

The Wiretap Act also prohibits a person or entity providing "electronic communication service" to "the public" from intentionally "divulg[ing] the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a). It is unclear whether the federal Government provides "electronic communication service" to "the public." It reasonably could be argued that an EINSTEIN 2.0 Participant does offer Web sites and other Internet-related services that enable the transmission of electronic communications to and from the public, qualifies as a provider of electronic communication service to the public. *See id.* § 2510(15) (defining "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communication service"); *Black's Law Dictionary* 1227 (6th ed. 1990) (defining public as "aggregate of the citizens"; "everybody"; "the community at large"). We need not decide the issue today, for even if the Government is a provider of electronic communication service to the public, we do not believe that EINSTEIN 2.0 operations run afoul of the prohibitions in the Wiretap Act on the divulging of the contents of wire and electronic communications.

We conclude that EINSTEIN 2.0 operations do not constitute an *unlawful* interception or divulging of the contents of Internet communications under the Wiretap Act for two reasons. First, where EINSTEIN 2.0 Participants obtain the consent of their employees through appropriate log-on banners or computer-user agreements, there would be no violation of the Wiretap Act. Second, there is a strong argument that the Government's EINSTEIN 2.0 operations are subject to the "rights or property" exception to the Wiretap Act. We also discuss, but do not decide, whether EINSTEIN 2.0 operations fall within the new "computer trespasser" exception to the prohibitions of the Wiretap Act.

1.

Under the Act, "[i]t shall not be unlawful . . . for a person acting under color of law to intercept a[n] . . . electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(c). Likewise, a person providing electronic communication service to the public "may divulge the contents of any such communication" either "to a person . . . authorized, or whose facilities are used, to forward such communications to its destination," *id.* § 2511(3)(b)(iii), or "with the lawful consent of the originator or any addressee or intended recipient of such communication," *id.* § 2511(3)(b)(ii). These exceptions take EINSTEIN 2.0 operations, if conducted consistent with the terms of the EINSTEIN 2.0 MOA, outside the scope of the prohibitions in the Wiretap Act.

The exception in section 2511(2)(c) applies to the interception of the contents of an Internet communication where an executive department or agency is a direct party to the communication, such as where an individual files a form with an agency through a Web site or responds online to a government survey. There is no violation of the Wiretap Act where "a person acting under color of law" intercepts an electronic communication provided that "one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(c). For purposes of section 2511(2)(c), DHS is "a person acting under color of law" in the course of conducting EINSTEIN 2.0 operations. *Id.* § 2510(6) (defining person to include any "agent" of the United States Government). *See Nardone v. United States*, 302 U.S. 379, 384 (1937) (government bound by wiretap laws because "the sovereign is embraced by general words of a statute intended to prevent injury"); *cf.* 18 U.S.C. § 2520(a) (2006) (plaintiff may recover civil damages from "a person or entity, other than the United States," which engaged in that violation). By entering into an MOA with DHS, an EINSTEIN 2.0 Participant has signaled its consent to the interception by EINSTEIN 2.0 sensors and DHS of the content of Internet communications to which it is a party. Therefore, DHS lawfully may intercept the contents of an EINSTEIN 2.0 Participant's Internet communications with individuals under the Wiretap Act. *Id.* § 2511(2)(c). For the same reason, it also is lawful for an EINSTEIN 2.0 Participant to divulge the contents of an Internet communication to DHS for the purposes of EINSTEIN 2.0 operations where an EINSTEIN 2.0 Participant is one of the addressees or recipients of the communication. *Id.* § 2511(3)(b)(ii) (person may divulge contents of communication "with the lawful consent of the originator or any addressee or intended recipient of such communication").

With respect to intercepting and divulging the contents of Internet communications involving Executive Branch employees and individuals outside the Executive Branch, we do not

believe that such actions would violate the prohibitions in the Wiretap Act. To begin with, EINSTEIN 2.0 operations do not unlawfully "divulge" the contents of Internet communications with Executive Branch employees, because the federal Government is "authorized," and its "facilities are used, to forward such communications to [their] destination." 18 U.S.C. § 2511(3)(b)(iii). Internet communications cannot get to or from Executive Branch employees at work without routing through the facilities of Federal Systems.

There also is no violation of either the interception or the divulging prohibitions of the Wiretap Act where one of the parties to a communication has given consent. *See* 18 U.S.C. § 2511(2)(c) ("prior consent" required for intercept); *id.* § 2511(3)(b)(ii) ("lawful consent" required for divulging). An EINSTEIN 2.0 Participant cannot consent to the interception of the contents of the communications of its employees on their behalf; rather, the consent of the employee who is the sender or the recipient of the communication is required. *See Television Surveillance Opinion*, 3 Op. O.L.C. at 67 (consent to surveillance is "not predicated on the consent of the owner of the pertinent property, but rather on the consent of the person to whom the targeted individual reveals his communications or activities"); *see also Caceres*, 440 U.S. at 750 ("[F]ederal statutes impose no restrictions on recording a conversation with the consent of one of the conversants."); *United States v. Barone*, 913 F.2d 46, 49 (2d Cir. 1990) (one-party consent obviates the need to obtain a court order under the Wiretap Act). As with any other person, an employee's consent under the Wiretap Act also must be provided voluntarily. *See United States v. Hernandez*, 93 F.3d 1493, 1500 (10th Cir. 1996). Here, an employee's valid, voluntary consent is expressly apparent from his clicking through the log-on banner or signing the computer-user agreement in order to access a Government-owned information system. *See supra* pp. 16-21; Memorandum for Ronald D. Lee, Associate Deputy Attorney General, from William Treanor, Deputy Assistant Attorney General, Office of Legal Counsel, *Re: Report of the Working Group on Access to Government Property (Second Draft)* at 5 (June 1, 2000) (consent exception in Wiretap Act satisfied where employee clicks through log-on banner acknowledging monitoring of electronic communications in order to access DOJ's computer network).

An Executive Branch employee's consent to interception or divulging of the contents of his Internet communications also may be implied where the "'circumstances indicat[e] that the [individual] knowingly agreed to the surveillance.'" *United States v. Van Poyck*, 77 F.3d 285, 292 (9th Cir. 1996) (quoting *United States v. Amen*, 831 F.2d 373, 378 (2d Cir. 1987) (federal inmate consented to interception of phone calls where notice that inmate calls were monitored was ubiquitous)). Under the Wiretap Act, "as in other settings, consent inheres where a person's behavior manifests acquiescence or a comparable voluntary diminution of his or her otherwise protected rights." *Griggs-Ryan v. Smith*, 904 F.2d 112, 116 (1st Cir. 1990) (tenant consented to landlord's recording of phone calls where tenant knew that all calls were being recorded); *accord United States v. Staves*, 383 F.3d 977, 981 (9th Cir. 2004) (party to communication impliedly consents to monitoring where circumstances "indicate that [he] knew that interception was likely and agreed to the monitoring"). Where "language or acts . . . tend to prove (or disprove) that a party knows of, or assents to, encroachments" on a routine expectation of privacy, that party has manifested his consent for purposes of the Wiretap Act. *Griggs-Ryan*, 904 F.2d at 117; *see Van Poyck*, 77 F.3d at 292 (similar).

Here, no Executive Branch employee who has read the model log-on banner or computer-user agreement (or a log-on banner or computer-user agreement with substantially equivalent terms) and who nonetheless has logged on to a Government-owned information system could reasonably claim not to have knowledge that monitoring, interception, and searches of his Internet communications would occur. The employee's use of Government-owned information systems despite that knowledge would establish voluntary consent to any such monitoring, interception, or search. *See supra* pp. 13, 16-21.[10] Therefore, we believe that EINSTEIN 2.0 operations would comply with the Wiretap Act as long as EINSTEIN 2.0 Participants consistently adopt, implement, and enforce the terms of appropriate log-on banners or computer-user agreements, as discussed in this memorandum.

2.

Even absent the consent of Executive Branch employees, there is a reasonable basis to conclude that the use of EINSTEIN 2.0 technology to protect Federal Systems comes within the express terms of the "rights or property" exception to the prohibitions in the Wiretap Act, 18 U.S.C. § 2511(2)(a)(i). The "rights or property" exception provides in relevant part that the prohibitions in the Act shall not apply to the "intercept, disclosure, or use" of an "electronic communication" by a "provider of a wire or electronic communication service . . . engaged in any activity which is a necessary incident to . . . the protection of the rights or property of the provider of that service." *Id.*

We believe that this provision may be applied to the Government here as a "provider" of "electronic communication service[s]" for its employees. Executive Branch departments and agencies provide the necessary computers, network infrastructure, facilities, and connectivity to the Internet that enable Executive Branch employees "to send or receive" electronic communications. 18 U.S.C. § 2510(15) (defining "electronic communication service"). The courts have held that to benefit from the rights or property exception, the electronic communication service provider's activities must protect the provider's own rights or property, and not those of any third party, such as a customer. *See, e.g.*, *Campiti v. Walonis*, 611 F.2d 387, 393 (1st Cir. 1979) (rights or property exception does not apply to a person who is not an agent of the telephone company for monitoring that "had nothing to do with telephone company equipment or rights"); *United States v. Auler*, 539 F.2d 642, 645-46 (7th Cir. 1976) (telephone companies intercepting communications under section 2511(2)(a)(i) may share those communications with the government only to the extent necessary to protect telephone company's rights or property). EINSTEIN 2.0 technology is owned, operated, and controlled by DHS, and we understand that it is to be used solely for the protection of the Government's rights and property in Federal Systems. *See supra* p. 3.

[10] Similarly, no reasonable person communicating directly with an agency of the federal Government through the Internet, such as by filing a form on an agency Web site, could claim not to know that his communication would be acquired by the Government. Indeed, that is the entire purpose of communicating with the Government. *See supra* p. 14. Hence, the individual impliedly would consent to the Government's interception of the contents of his communication. *See Caller ID Opinion*, 20 Op. O.L.C. at 320 & n.13 (dialing 911 constitutes implicit consent to Government's direct monitoring of an emergency call).

The legislative history of the rights or property exception in the Wiretap Act arguably speaks only to the efforts of telephone companies to monitor calls in order to prevent callers from using "blue boxes" to avoid paying for long-distance telephone calls. *See* S. Rep. No. 90-1097, at 67 (1967), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2182. Nevertheless, we believe that "the plain meaning of Congress'[s] language" in the "rights or property" exception includes EINSTEIN 2.0 operations "within its ambit." *United States v. Savage*, 564 F.2d 728, 731 (5th Cir. 1977). The courts have construed the "necessary" language in the Wiretap Act provision "to impose a standard of reasonableness upon" the provider's activities to protect his rights or property. *United States v. Harvey*, 540 F.2d 1345, 1351 (8th Cir. 1976); *see, e.g.*, *United States v. McLaren*, 957 F. Supp. 215, 220 (M.D. Fla. 1997) (similar). As in the Fourth Amendment context, reasonableness is "assessed under the facts of each case." *Harvey*, 540 F.2d at 1352 n.9. The "rights or property" exception does not strictly *require* "minimization" of the acquisition of communication contents by a provider, *McLaren*, 957 F. Supp. at 220, but a provider's activities are reasonable under the exception where they involve only "minimal interception" of communications. *Harvey*, 540 F.2d at 1351.

We believe that the Government's use of EINSTEIN 2.0 technology to detect intrusions and exploitations against Federal Systems is reasonably necessary to protect the federal Government's rights with respect to its exclusive use of Federal Systems and its property interests in the integrity and security of its networks and data. For the reasons we have noted already, *see supra* pp. 18-21, we believe that EINSTEIN 2.0 operations would involve the minimal acquisition and storage of communications necessary to detect malicious network activity directed against Federal Systems. EINSTEIN 2.0 operations are limited to the detection and storing of data packets containing only malicious computer code associated with computer intrusions and exploitations, and are reasonably designed to protect Federal Systems without acquiring any additional content of Internet communications that is unrelated to that goal. Thus, EINSTEIN 2.0 operations are appropriately limited in scope to what is reasonably necessary to protect governmental rights and property against computer intrusions and exploitations. *See Harvey*, 540 F.2d at 1351 (recording of limited portion of phone calls to identify use of technology to evade paying for long-distance calls is "reasonable"); *United States v. Freemen*, 524 F.2d 337, 341 (7th Cir. 1975) (taping of conversations for no more than two minutes and only when blue box was in use was "necessary and in line with the minimal invasion of privacy contemplated by the statute"); *cf. Auler*, 539 F.2d at 646 (monitoring and recording of all calls, regardless whether made using a blue box, acquired "far more information" than the telephone company "needed to protect its interests"); *McLaren*, 957 F. Supp. at 220 (interception, recording, and disclosure of complete phone calls "having nothing whatever to do" with abuse of telephone company's service is unreasonable because those actions "could not possibly be 'necessary'" to protecting the company's rights).

Therefore, even absent employee consent, there is a strong basis in the text of the "rights or property" exception to the Wiretap Act to believe that the Government's activities under EINSTEIN 2.0 would not violate the prohibitions in the Wiretap Act. That being said, however, there are very few cases applying the rights or property exception since the mid-1970s, and almost none involving computer networks, the Internet, or defenses against cyber intrusions and exploitations, and none involving the Government in protecting its own rights or property, as opposed to a private communications provider protecting its private property. Accordingly, we

believe there is some uncertainty regarding how the courts would view a defense of EINSTEIN 2.0 operations based upon the "rights or property" exception to the Wiretap Act.

3.

Finally, we discuss briefly the "computer trespasser" exception in the Wiretap Act, 18 U.S.C. § 2511(2)(i), which was added to the Wiretap Act by section 217 of the USA PATRIOT Act, *see* Public Law No. 107-56, 115 Stat. 272, 291 (2001). Section 2511(2)(i) permits "a person acting under color of law" to "intercept" the contents of "wire or electronic communications of a computer trespasser transmitted to, through, or from [a] protected computer" on four conditions: First, "the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer." Second, "the person acting under color of law is lawfully engaged in an investigation." Third, "the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation." And fourth, "such interception does not acquire communications other than those transmitted to or from the computer trespasser." 18 U.S.C. § 2511(2)(i)(I)-(IV). The phrase "protected computer" has the same definition as in 18 U.S.C. § 1030(e)(2), *see id.* § 2510(20) (defining "protected computer"), which includes the Government-issued computers of EINSTEIN 2.0 Participants at issue here. "Computer trespasser" is defined to mean "a person who accesses a protected computer without authorization" and "does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer." *Id.* § 2510(21)(A) & (B).

We need not discuss the first three requirements of the computer trespasser exception. Even assuming that EINSTEIN 2.0 operations satisfy these requirements, it is questionable that EINSTEIN 2.0 operations satisfy the final requirement. The computer trespasser exception is applicable only if interception of the contents of communications "does not acquire communications other than those transmitted to or from the computer trespasser." 18 U.S.C. § 2511(2)(i)(IV). We understand that EINSTEIN 2.0 technology is designed to detect and to store only packets containing malicious computer code associated with a signature. Accordingly, it could be argued that it would not acquire communications other than the malicious code sent over the Internet by computer trespassers, as defined in section 2510(21). However, EINSTEIN 2.0 technology also can acquire the contents of communications to or from persons who do not satisfy the definition of "computer trespasser." To take just one example, an Executive Branch employee—even one who intentionally includes malicious computer code in his Internet communications at work—does not appear to be a "computer trespasser" within the scope of the definition. *See id.* § 2510(21)(B) (defining "computer trespasser" to exclude a "person known by the owner or operator of the protected computer to have an existing contractual relationship . . . for access to all or part of the protected computer").[11] EINSTEIN 2.0 operations, however, nonetheless would acquire the contents of their communications.

[11] That does not mean that the Government would be prohibited from acquiring the communications of an employee or contractor who intentionally incorporates malicious code in their Internet communications. Rather, some other statutory exception—such as consent or the rights or property exception—may authorize that result.

We do not decide, however, whether the computer trespasser exception would or would not apply to EINSTEIN 2.0 operations. In light of the other legal justifications for EINSTEIN 2.0 operations under the Wiretap Act, we need not rely upon this provision.

B.

We next consider whether the provisions in title I of FISA, which govern the conduct of "electronic surveillance" within the United States, and in revised title VII of FISA, which govern, among other things, the acquisition of foreign intelligence information from United States persons outside the United States, apply to the deployment, testing, and use of EINSTEIN 2.0 technology. We conclude that they do not, provided that EINSTEIN 2.0 Participants obtain the consent of their employees through the terms of log-on banners or computer-user agreements, as discussed throughout this memorandum.

1.

Under 50 U.S.C.A. § 1809(a)(1) (West 2008), it is a felony for a person acting "under color of law" to engage intentionally in "electronic surveillance" as defined in title I of FISA, *see* 50 U.S.C. § 1801(f), "except as authorized" by FISA, the Wiretap Act, the SCA, the Pen/Trap Act, or any other "express statutory authorization that is an additional exclusive means for conducting electronic surveillance" under 50 U.S.C.A. § 1812(b) (West 2008). *See also id.* § 1810 (West 2008) (establishing civil penalties for violations of section 1809(a)(1). As we have established in Part III.A., EINSTEIN 2.0 operations would not be prohibited by the Wiretap Act. Thus, it could be argued that they are "authorized" under the Wiretap Act. On this view, FISA does not govern activity that is expressly permitted under provisions in the Wiretap Act, such as activity falling within the terms of the consent or the rights or property exception. *Cf. Freemen*, 524 F.2d at 340 & n.5 (phrase "[e]xcept as authorized by [the Wiretap Act]" in 47 U.S.C. § 605(a) (1970) "permits" telephone companies to protect their rights or property under section 2511(2)(a)(i) notwithstanding any otherwise applicable terms of section 605(a)). Accordingly, EINSTEIN 2.0 operations permitted under the rights or property exception of the Wiretap Act would be authorized notwithstanding the electronic surveillance provisions of FISA (and notwithstanding the absence of a rights or property exception in FISA).

There is much to recommend that view, although the better reading of "authorized" may be that the term refers to orders obtained under the procedures of the Wiretap Act, the SCA, the Pen/Trap Act, or another covered statute, rather than to activities that merely are not prohibited by those statutes. *Cf. United States v. Keen*, 508 F.2d 986, 988 (9th Cir. 1974) ("Section 2511(2)(c) is worded as an exception to [the] general prohibition of judicially non-authorized wire taps, not as a positive authorization of such taps."). We need not and do not resolve this issue today. Rather, we assume for the purposes of this memorandum that title I of FISA applies to the deployment, testing, and use of EINSTEIN 2.0 technology if those actions constitute "electronic surveillance" within the meaning of 50 U.S.C. § 1801(f).

Section 1801(f) sets forth four separate definitions of "electronic surveillance." They are as follows:

> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communications sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
>
> (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;
>
> (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
>
> (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

50 U.S.C. § 1801(f)(1)-(4). EINSTEIN 2.0 operations that scan, acquire, and store copies of data packets containing malicious computer code from Federal Systems Internet Traffic constitute an "acquisition" of the "contents" of a communication. *Id.* § 1801(n) (defining "contents" to include "any information concerning the identity of the parties to . . . communications or the existence, substance, purport, or meaning of that communication").

Nevertheless, paragraphs (1) and (3) of section 1801(f) do not apply to EINSTEIN 2.0 operations. Those operations do not constitute electronic surveillance under section 1801(f)(1), because EINSTEIN 2.0 sensors generally would not target any "particular, known United States person" in the United States. Nor do EINSTEIN 2.0 operations constitute electronic surveillance within the meaning of section 1801(f)(3), because the EINSTEIN 2.0 sensors do not acquire the contents of any "radio communication." As explained *supra* in Part I, EINSTEIN 2.0 sensors are to scan only a mirror copy of Federal Systems Internet Traffic created as that traffic passes through the facilities located at the Government's TICs. Furthermore, even if section 1801(f)(1) and section 1801(f)(3) did apply to EINSTEIN 2.0 operations, the use of EINSTEIN 2.0 technology still does not constitute "electronic surveillance" under those definitions, because the use of those sensors does not implicate "a person's reasonable expectation of privacy." *See supra* pp. 7-14 and *infra* p. 30.

That leaves section 1801(f)(2) and (4). Section 1801(f)(2) applies to EINSTEIN 2.0 operations only if EINSTEIN 2.0 technology acquires the contents of "wire communication[s],"

which FISA defines as "any communication while it is being carried by a wire, cable, or other like connection furnished or operated by . . . a common carrier . . . providing or operating such facilities for the transmission of interstate or foreign communications." 50 U.S.C. § 1801(l); *see* H.R. Rep. No. 95-1283, at 66-67 (1978) (communications are wire communications "only when they are carried by a wire furnished or operated by a common carrier"). FISA does not define the term "common carrier." We need not decide whether EINSTEIN 2.0 operations acquire the contents of communications while being carried by the wire facilities of a common carrier. Even if they do, the use of EINSTEIN 2.0 technology does constitute electronic surveillance under section 1801(f)(2) as long as the Government obtains "the consent of any party" to a communication to acquire the contents of that communication. 50 U.S.C. § 1801(f)(2).

Because the consent exception in section 1801(f)(2) concerns the same subject matter—consent of a party to a communication—as section 2511(2)(c), we construe the two provisions *in pari materia*. *See Wachovia Bank, N.A. v. Schmidt*, 126 S. Ct. 941, 950 (2006) (statutes addressing a similar subject matter should be read "as if they were one law") (internal quotation marks omitted); *Authority of USDA to Award Monetary Relief for Discrimination*, 18 Op. O.L.C. 52, 69 (1994) ("Statutes addressing the same subject matter—that is, statutes '*in pari materia*'—should be construed together."). That construction is consistent with the stated views of the Senate Select Committee on Intelligence and the Senate Committee on the Judiciary in their respective committee reports on the legislation that ultimately would become FISA. *See* S. Rep. No. 95-604, pt. I, at 35 (1978) (definition of electronic surveillance "has an explicit exception where any party has consented to the interception. This is intended to perpetuate the existing law regarding consensual interceptions found in 18 U.S.C. § 2511(2)(c)."), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3936-37; S. Rep. No. 95-701, at 37 (1978) (same), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4006. Accordingly, for the same reasons already noted above with respect to the Wiretap Act, we believe that the Government could obtain valid consent under section 1801(f)(2) through consistent and actual use of log-on banners or computer-user agreements. *See United States v. Missick*, 875 F.2d 1294, 1299 (7th Cir. 1989) (section 1801(f)(2) does not apply to acquisition of content of telephone calls where one of the parties consented).

For that same reason, we do not believe that EINSTEIN 2.0 operations constitute "electronic surveillance" under section 1801(f)(4). It is plain that the use of EINSTEIN 2.0 technology constitutes "the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information." 50 U.S.C. § 1801(f)(4). But regardless whether that technology would acquire the contents of communications "other than from" the wire facilities of a common carrier, EINSTEIN 2.0 operations would not fall within the scope of section 1801(f)(4). As long as EINSTEIN 2.0 Participants consistently adopt, implement, and enforce the use of appropriate log-on banners or computer-user agreements as discussed in this memorandum, EINSTEIN 2.0 technology would not acquire the contents of Internet communications under circumstances where there is a "reasonable expectation of privacy" and a warrant "would be required for law enforcement purposes." *See supra* pp. 7-14, 23-25; *see also Interception of Radio Communication*, 3 Op. O.L.C. 240, 241 (1979) (phrase "reasonable expectation of privacy" in FISA incorporates "the standard of constitutionally protected privacy interests"); H.R. Rep. No. 95-1283, pt. 1, at 53 (1978) (under section 1801(f)(4) "the acquisition of information [must] be under circumstances in which a person has a constitutionally protected right of privacy. There may be no such right in those situations where

the acquisition is consented to by at least one party to the communication"); S. Rep. No. 95-701, at 37 (1978) (same).

Therefore, EINSTEIN 2.0 operations would not constitute "electronic surveillance" under title I of FISA as long as EINSTEIN 2.0 Participants consistently adopt, implement, and enforce the terms of appropriate log-on banners or computer-user agreements, as discussed in this memorandum.

2.

For the same reasons, we do not believe that the use of EINSTEIN 2.0 technology with respect to the Federal Systems Internet Traffic of Executive Branch employees outside the United States, such as (hypothetically) employees of the Department of State or the Central Intelligence Agency, implicates revised title VII of FISA. As applicable here, section 703(a)(1) of FISA provides that the Foreign Intelligence Surveillance Court ("FISC") shall have jurisdiction over the "the targeting of a United States person reasonably believed to be located outside the United States to acquire foreign intelligence information if the acquisition constitutes electronic surveillance" under FISA. 50 U.S.C.A. § 1881b(a)(1) (West 2008). And section 704(a)(2) of FISA generally prohibits elements of the Intelligence Community from "intentionally target[ing], for the purpose of acquiring foreign intelligence information, a United States person reasonably believed to be located outside the United States in circumstances where [the person] has a reasonable expectation of privacy and where a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes." *Id.* § 1881c(a)(2).

We have no reason to believe that EINSTEIN 2.0 operations generally would involve the intentional targeting of any United States person employed by an EINSTEIN 2.0 Participant outside the United States in order to acquire "foreign intelligence information" as defined in 50 U.S.C. § 1801(e). Even assuming for the sake of argument that EINSTEIN 2.0 operations would satisfy those requirements, we do not believe those operations would satisfy the other jurisdictional requirements in sections 1881b(a)(1) or 1881c(a)(2), provided that EINSTEIN 2.0 Participants employing United States persons outside the United States consistently adopt, implement, and enforce appropriate notice and consent procedures, as discussed in this memorandum. In that circumstance, there would be no "electronic surveillance" as defined in section 1801(f)(1)-(4), and, thus, section 1881b(a)(1) would be inapplicable. *See supra* pp. 28-31. Likewise, there would be no reasonable expectation of privacy and a warrant would not be required for law enforcement purposes for either of two reasons: there would be no search under the Fourth Amendment, *see supra* pp. 7-14, or there would be proper consent, thus obviating the need for a warrant and probable cause, *see supra* pp. 13, 16-21. Under either rationale (or both), the prohibition in section 1881c(a)(2) would not apply. Therefore, we do not believe that EINSTEIN 2.0 operations would be subject to revised title VII of FISA.

C.

We also conclude that the relevant provisions of the Stored Communications Act would not apply to EINSTEIN 2.0 operations, provided that EINSTEIN 2.0 Participants consistently

adopt, implement, and enforce the terms of appropriate log-on banners or computer-user agreements, as discussed in this memorandum. As relevant here, the SCA prohibits a person or entity "providing an electronic communication service to the public" from knowingly "divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1) (2006). As already noted with respect to the Wiretap Act, it is unclear that the federal Government—which does offer Web sites and other Internet-related services that enable the transmission of electronic communications to and from the public—qualifies as a provider of electronic communication service to the public under the SCA. *See supra* p. 22. The matter is far from settled. *Compare Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041, 1042-43 (N.D. Ill. 1998) (computer system of partnership used to communicate with third parties does not provide electronic communication service to the public within the meaning of the SCA), *with Bohach v. City of Reno*, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (City of Reno is an "electronic communication service provider" under the SCA because it provides the terminals, computers, pages, and software that enables its own personnel to send and to receive electronic communications). We need not decide the issue, for even if the Government is a provider of electronic communication service to the public, we do not believe that EINSTEIN 2.0 operations would run afoul of the SCA.

EINSTEIN 2.0 operations would implicate the prohibition in section 2702(a)(1) if the temporary mirroring of all Federal Systems Internet Traffic of EINSTEIN 2.0 Participants divulges the content of an electronic communication "while in electronic storage." The SCA defines "electronic storage" to mean:

> (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
>
> (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

Id. § 2510(17)(A) & (B). The courts have interpreted section 2510(17)(A) to apply only to an electronic communication stored temporarily on a provider's server pending delivery of the communication to the recipient. *See, e.g.*, *In re DoubleClick, Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 511-12 (S.D.N.Y. 2001). As noted in Part I, *supra* p. 4, EINSTEIN 2.0 technology does not have any effect upon the transmission of wire or electronic communications to their intended recipients. Rather, EINSTEIN 2.0 operations will make a mirror copy of every packet in Federal Systems Internet Traffic and will scan that copy to detect known signatures. This copy is "temporary" storage of communications "incidental" to their transmission, in the sense that the storage is related to the transmission of those communications. But arguably it is not "intermediate" in the process of that transmission, because the temporary copy is not created as part of a step in the chain of transmitting the communication to its intended recipient. Rather, the copy is made for the separate purpose of enabling EINSTEIN 2.0 sensors to detect malicious computer code embedded in Federal Systems Internet Traffic. Indeed, the EINSTEIN 2.0 scanning process occurs out-of-line from the transmission process, even if it is related to the in-line transmission of Federal Systems Internet Traffic.

Nor do we understand that EINSTEIN 2.0 operations would divulge the content of any communication while in storage "for purposes of backup protection" within the meaning of section 2510(17)(B), even under a broader reading of "backup protection" than DOJ has embraced in litigating the scope of that provision. *See Theofel v. Farey Jones*, 341 F.3d 978, 985 (9th Cir. 2003) (backup protection means "storing a message on a service provider's server after delivery to provide a second copy of the message in the event that the user needs to download it again"). Because the EINSTEIN 2.0 sensors scan a mirror copy of Federal Systems Internet Traffic for the purpose of detecting malicious computer code, there is no routing of the contents of any communication stored by an ISP for purposes of backup protection. It is true that EINSTEIN 2.0 technology would store data packets containing malicious computer code for later review by DHS analysts. But the "purpose" of any storage and subsequent review by analysts of blocked data packets would be to prevent intrusions and exploitations against Federal Systems, and not "to provide a second copy of the message in the event that the user needs to download it again." *Id.* at 985. Therefore, we have no reason to believe that EINSTEIN 2.0 operations would divulge the contents of communications stored for backup protection.

Even if section 2702(a)(1) would apply to EINSTEIN 2.0 operations, scanning Federal Systems Internet Traffic for malicious computer code would fall within the SCA's consent exception in 18 U.S.C. § 2702(b)(3) as long as EINSTEIN 2.0 Participants consistently adopt, implement, and enforce the terms of appropriate log-on banners or computer-user agreements, as discussed in this memorandum. Section 2702(b)(3) states in relevant part that an electronic communication service provider "may divulge the contents of a communication . . . with the lawful consent of the originator or an addressee or intended recipient of such communication." *Id.*; *see also id.* § 2702(c)(2) (provider may divulge information pertaining to subscriber or customer of electronic communication service, but not the contents of that communication, "with the lawful consent of the customer or subscriber"). We have interpreted a similar consent exception in 18 U.S.C. § 2703(c)(1)(B)(iii) (2006), which states that a provider shall divulge a record pertaining to the identity of a subscriber or customer—but not the contents of a communication—to a governmental entity that "has the consent" of the customer or subscriber, *in pari materia* with the consent exception in the Wiretap Act. *See Caller ID Opinion*, 20 Op. O.L.C. at 319 & n.12 (interpreting consent exception in section 2703(c)(1)(B)(iii) in accord with the consent exception in the Wiretap Act). We also construe the consent exception in section 2702(b)(3)—which is even more closely analogous to the consent exception in section 2511(2)(c) than is section 2703(c)(1)(B)(iii)—*in pari materia* with section 2511(2)(c). *See supra* p. 30. For the reasons already noted with respect to the consent exception in the Wiretap Act, *see supra* pp. 23-25, to the extent the SCA applies to EINSTEIN 2.0 operations, we believe that the Government could obtain proper consent under section 2702(b)(3) and (c)(2) through the consistent and actual use of log-on banners or computer-user agreements.[12]

[12] EINSTEIN 2.0 operations also may fall within the "rights or property" exceptions to the SCA, *see* 18 U.S.C. § 2702(b)(5), (c)(3). The SCA's "rights or property" exceptions are substantively similar to the parallel exception in the Wiretap Act. The SCA's first rights or property provision states that a provider of electronic communication service to the public may divulge the contents of a stored communication "as may be necessarily incident . . . to the protection of the rights or property of the provider of that service." 18 U.S.C. § 2702(b)(5). Another provision in the SCA permits a provider of electronic communication service to the public to disclose non-content information regarding a subscriber or a customer "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." *Id.* § 2702(c)(3). In light of the similarities in wording and

D.

Finally, we conclude that the Pen/Trap Act would not apply to EINSTEIN 2.0 operations where EINSTEIN 2.0 Participants consistently adopt, implement, and enforce the terms of appropriate log-on banners or computer-user agreements, as discussed in this memorandum. Section 3121(a) of title 18, United States Code, provides that "[e]xcept as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or" FISA. 18 U.S.C. § 3121(a) (2006). As relevant here, the statute defines a "pen register" as a "device . . . which records or decodes . . . routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication." *Id.* § 3127(3) (2006). And a "trap and trace device" means "a device . . . which captures the incoming electronic or other impulses which identify . . . routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication." *Id.* § 3127(4).[13]

We assume for the purposes of this memorandum that the use of EINSTEIN 2.0 technology would fall within the definitions of both a pen register and a trap and trace device, because they can both "record" and "capture," 18 U.S.C. § 3127(3) and (4), information that identifies routing, addressing, and signaling information for data packets that are part of Federal Systems Internet Traffic. *See supra* pp. 3-4, 7. Hence, absent an exception, we assume that the Government would be required to obtain a court order before the deployment, testing, and use of EINSTEIN 2.0 technology. *See* 18 U.S.C. § 3123 (2006).

As with the Wiretap Act, FISA, and the SCA, obtaining the valid consent of Executive Branch employees also exempts EINSTEIN 2.0 operations from any applicable requirement of the Pen/Trap Act. Section 3121(a) "does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service . . . where the

---

subject matter between the SCA's rights or property exceptions and the Wiretap Act's parallel provision, we construe them *in pari materia*. *See supra* pp. 30 & 33.

A crucial difference, however, between the "rights or property" exceptions in the SCA and the one in the Wiretap Act is that the SCA provisions apply only to a provider of electronic communication service *to the public*, whereas the Wiretap Act provision applies to *any* provider of such service, whether to the public or otherwise. As we noted, it is debatable whether the Government is a "provider" of electronic communication service to the public under the SCA. *See supra* pp. 22 & 32. Assuming that the Government is a public provider of electronic communication service, the SCA's rights or property exceptions apply to any action under EINSTEIN 2.0 divulging the contents of stored electronic communications or non-content information concerning a subscriber or a customer that is reasonably necessary to protect Federal Systems. *See supra* pp. 25-27. Of course, if the Government is not a public provider, then the provisions of the SCA do not apply to it in any event.

[13] Title III of FISA also establishes a statutory basis for the Government to obtain an authorization from the FISC to install a pen register or a trap and trace device in order to acquire certain foreign intelligence information. *See* 50 U.S.C. §§ 1841-1846 (2000 & Supp. V 2005). Under FISA, the terms "pen register" and "trap and trace device" have the same meanings as used in 18 U.S.C. § 3127(3) and (4). *See* 50 U.S.C. § 1841(2).

consent of the user of that service has been obtained." 18 U.S.C. § 3121(b)(3).[14] We believe that an EINSTEIN 2.0 Participant providing Internet service to its employees through Government-owned information systems and its Federal Systems would qualify as a "provider of electronic . . . communication service" within the meaning of the Pen/Trap Act. *See supra* pp. 25; 18 U.S.C. § 2510(15). Accordingly, the Government would be exempt from the prohibitions of the Pen/Trap Act with respect to EINSTEIN 2.0 operations where the "consent" of the "user[s]" of their electronic communication service "has been obtained." With respect to both entities, we believe that the "user" whose consent needs to be obtained is the Executive Branch employee using a Government-owned computer at an IP address that is subject to EINSTEIN 2.0 operations. For the same reasons discussed above we believe that EINSTEIN 2.0 Participants could obtain proper consent from their employees under section 3121(b)(3) through the consistent adoption, implementation, and enforcement of appropriate log-on banners or computer-user agreements, as discussed in this memorandum. Therefore, we conclude that the deployment, testing, and use of EINSTEIN 2.0 technology would not constitute the unauthorized installation or use of a pen register or a trap and trace device under 18 U.S.C. § 3121(a).[15]

/s /

STEVEN G. BRADBURY
Principal Deputy Assistant Attorney General

[14] The consent exception in section 3121(b)(3) also applies to the provisions in FISA authorizing the installation or use of such devices to acquire foreign intelligence information.

[15] EINSTEIN 2.0 operations also may fall within the "rights or property" exception to the Pen/Trap Act. Section 3121(b)(1) provides that the prohibitions of that Act do not apply with respect to the use of such technology "by a provider of electronic or wire communication service . . . relating to . . . the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service." 18 U.S.C. § 3121(b)(1).

We believe there is a strong argument that EINSTEIN 2.0 operations are subject to this "rights or property" exception. The rights or property exception in the Pen/Trap Act is more expansive than the parallel provisions in the Wiretap Act and the SCA. There is no requirement under the Pen/Trap Act provision that the action of a provider be "necessary" to protecting its rights or property. Furthermore, the Pen/Trap Act provision also permits a provider to protect not only its own rights or property, but also its users against "abuse of service or unlawful use of service." 18 U.S.C. § 3121(b)(1). Accordingly, under EINSTEIN 2.0 operations the Government is protecting the Executive Branch "users" of the Internet service and the Government's own rights and property. For these reasons and the reasons noted with respect to the narrower exception in the Wiretap Act, *see supra* pp. 25-27, we believe the rights or property exception to the Pen/Trap Act provides an additional basis to believe that EINSTEIN 2.0 operations are consistent with the Pen/Trap Act.

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

Plaintiff's Exhibit 26

~~TOP SECRET//SI//NOFORN//20320108~~

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT
2011 JUN 28 PM 3:56
LEEANN FLYNN HALL
CLERK OF COURT

EXHIBIT B

MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED

(U) Section 1 - Applicability and Scope

(U) These National Security Agency (NSA) minimization procedures apply to the acquisition, retention, use, and dissemination of information, including non-publicly available information concerning unconsenting United States persons, that is acquired by targeting non-United States persons reasonably believed to be located outside the United States in accordance with section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA or "the Act").

(U) If NSA determines that it must take action in apparent departure from these minimization procedures to protect against an immediate threat to human life (e.g., force protection or hostage situations) and that it is not feasible to obtain a timely modification of these procedures, NSA may take such action immediately. NSA will report the action taken to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which will promptly notify the Foreign Intelligence Surveillance Court of such activity.

~~(S//NF)~~ Nothing in these procedures shall restrict NSA's performance of lawful oversight functions of its personnel or systems, or lawful oversight functions of the Department of Justice's National Security Division, Office of the Director of National Intelligence, or the applicable Offices of the Inspectors General. Additionally, nothing in these procedures shall restrict NSA's ability to conduct vulnerability or network assessments using information acquired pursuant to section 702 of the Act in order to ensure that NSA systems are not or have not been compromised. Notwithstanding any other section in these procedures, information used by NSA to conduct vulnerability or network assessments may be retained for one year solely for that limited purpose. Any information retained for this purpose may be disseminated only in accordance with the applicable provisions of these procedures.

(U) For the purposes of these procedures, the terms "National Security Agency" and "NSA personnel" refer to any employees of the National Security Agency/Central Security Service ("NSA/CSS" or "NSA") and any other personnel engaged in Signals Intelligence (SIGINT) operations authorized pursuant to section 702 of the Act if such operations are executed under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA).

(U) Section 2 - Definitions

(U) In addition to the definitions in sections 101 and 701 of the Act, the following definitions will apply to these procedures:

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~20320108~~

(a) (U) Acquisition means the collection by NSA or the Federal Bureau of Investigation (FBI) through electronic means of a non-public communication to which it is not an intended party.

(b) (U) Communications concerning a United States person include all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly available information about the person.

(c) (U) Communications of a United States person include all communications to which a United States person is a party.

(d) (U) Consent is the agreement by a person or organization to permit the NSA to take particular actions that affect the person or organization. To be effective, consent must be given by the affected person or organization with sufficient knowledge to understand the action that may be taken and the possible consequences of that action. Consent by an organization will be deemed valid if given on behalf of the organization by an official or governing body determined by the General Counsel, NSA, to have actual or apparent authority to make such an agreement.

(e) (U) Foreign communication means a communication that has at least one communicant outside of the United States. All other communications, including communications in which the sender and all intended recipients are reasonably believed to be located in the United States at the time of acquisition, are domestic communications.

(f) (U) Identification of a United States person means (1) the name, unique title, or address of a United States person; or (2) other personal identifiers of a United States person when appearing in the context of activities conducted by that person or activities conducted by others that are related to that person. A reference to a product by brand name, or manufacturer's name or the use of a name in a descriptive sense, e.g., "Monroe Doctrine," is not an identification of a United States person.

(g) ~~(TS//SI//NF)~~ Internet transaction, for purposes of these procedures, means an Internet communication that is acquired through NSA's upstream collection techniques. An Internet transaction may contain information or data representing either a discrete communication [redacted] or multiple discrete communications [redacted]

(h) (U) Processed or processing means any step necessary to convert a communication into an intelligible form intended for human inspection.

(i) (U) Publicly available information means information that a member of the public could obtain on request, by research in public sources, or by casual observation.

(j) (U) Technical data base means information retained for cryptanalytic, traffic analytic, or signal exploitation purposes.

(k) (U) United States person means a United States person as defined in the Act. The following guidelines apply in determining whether a person whose status is unknown is a United States person:

(1) (U) A person known to be currently in the United States will be treated as a United States person unless positively identified as an alien who has not been admitted for permanent residence, or unless the nature or circumstances of the person's communications give rise to a reasonable belief that such person is not a United States person.

(2) (U) A person known to be currently outside the United States, or whose location is unknown, will not be treated as a United States person unless such person can be positively identified as such, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person.

(3) (U) A person who at any time has been known to have been an alien admitted for lawful permanent residence is treated as a United States person. Any determination that a person who at one time was a United States person (including an alien admitted for lawful permanent residence) is no longer a United States person must be made in consultation with the NSA Office of General Counsel.

(4) (U) An unincorporated association whose headquarters or primary office is located outside the United States is presumed not to be a United States person unless there is information indicating that a substantial number of its members are citizens of the United States or aliens lawfully admitted for permanent residence.

(U) Section 3 - Acquisition and Handling - General

(a) (U) Acquisition

(U) The acquisition of information by targeting non-United States persons reasonably believed to be located outside the United States pursuant to section 702 of the Act will be effected in accordance with an authorization made by the Attorney General and Director of National Intelligence pursuant to subsection 702(a) of the Act and will be conducted in a manner designed, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the acquisition.

(b) (U) Monitoring, Recording, and Handling

(1) (U) Personnel will exercise reasonable judgment in determining whether information acquired must be minimized and will destroy inadvertently acquired communications of or concerning a United States person at the earliest practicable point at which such communication can be identified either: as clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information); or, as not containing evidence of a crime which may be

disseminated under these procedures. Except as provided for in subsection 3(c) below, such inadvertently acquired communications of or concerning a United States person may be retained no longer than five years from the expiration date of the certification authorizing the collection in any event.

(2) (U) Communications of or concerning United States persons that may be related to the authorized purpose of the acquisition may be forwarded to analytic personnel responsible for producing intelligence information from the collected data. Such communications or information may be retained and disseminated only in accordance with Sections 3, 4, 5, 6, and 8 of these procedures.

(3) (U//~~FOUO~~) As a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime for purposes of assessing how the communication should be handled in accordance with these procedures.

(4) (U) Handling of Internet Transactions Acquired Through NSA Upstream Collection Techniques

a. (~~TS//SI//NF~~) NSA will take reasonable steps post-acquisition to identify and segregate through technical means Internet transactions that cannot be reasonably identified as containing single, discrete communications where: the active user of the transaction (i.e., the electronic communications account/address/identifier used to send or receive the Internet transaction to or from a service provider) is reasonably believed to be located in the United States; or the location of the active user is unknown.

1. (~~TS//SI//NF~~) Notwithstanding subsection 3(b)(4)a. above, NSA may process Internet transactions acquired through NSA upstream collection techniques in order to render such transactions intelligible to analysts.

2. (~~TS//SI//NF~~) Internet transactions that are identified and segregated pursuant to subsection 3(b)(4)a. will be retained in an access-controlled repository that is accessible only to NSA analysts who have been trained to review such transactions for the purpose of identifying those that contain discrete communications as to which the sender and all intended recipients are reasonably believed to be located in the United States.

(a) (~~TS//SI//NF~~) Any information contained in a segregated Internet transaction (including metadata) may not be moved or copied from the segregated repository or otherwise used for foreign intelligence purposes unless it has been determined that the transaction does not contain any discrete communication as to which the sender and all intended recipients are reasonably believed to be located in the United States. Any Internet transaction that is identified and segregated pursuant to subsection

3(b)(4)a. and is subsequently determined to contain a discrete communication as to which the sender and all intended recipients are reasonably believed to be located in the United States will be handled in accordance with Section 5 below.

(b) (U//~~FOUO~~) Any information moved or copied from the segregated repository into repositories more generally accessible to NSA analysts will be handled in accordance with subsection 3(b)(4)b. below and the other applicable provisions of these procedures.

(c) (U//~~FOUO~~) Any information moved or copied from the segregated repository into repositories more generally accessible to NSA analysts will be marked, tagged, or otherwise identified as having been previously segregated pursuant to subsection 3(b)(4)a.

3. ~~(TS//SI//NF)~~ Internet transactions that are not identified and segregated pursuant to subsection 3(b)(4)a. will be handled in accordance with subsection 3(b)(4)b. below and the other applicable provisions of these procedures.

b. (U) NSA analysts seeking to use (for example, in a FISA application, intelligence report, or section 702 targeting) a discrete communication within an Internet transaction that contains multiple discrete communications will assess whether the discrete communication: 1) is a communication as to which the sender and all intended recipients are located in the United States; and 2) is to, from, or about a tasked selector, or otherwise contains foreign intelligence information.

1. ~~(TS//SI//NF)~~ If an NSA analyst seeks to use a discrete communication within an Internet transaction that contains multiple discrete communications, the analyst will first perform checks to determine the locations of the sender and intended recipients of that discrete communication to the extent reasonably necessary to determine whether the sender and all intended recipients of that communication are located in the United States. If an analyst determines that the sender and all intended recipients of a discrete communication within an Internet transaction are located in the United States, the Internet transaction will be handled in accordance with Section 5 below.

2. (U) If an NSA analyst seeks to use a discrete communication within an Internet transaction that contains multiple discrete communications, the analyst will assess whether the discrete communication is to, from, or about a tasked selector, or otherwise contains foreign intelligence information.

(a) (U) If the discrete communication is to, from, or about a tasked selector, any U.S. person information in that communication will be handled in accordance with the applicable provisions of these procedures.

(b) (U) If the discrete communication is not to, from, or about a tasked selector but otherwise contains foreign intelligence information, and the discrete communication is not to or from an identifiable U.S. person or a person reasonably believed to be located in the United States, that communication (including any U.S. person information therein) will be handled in accordance with the applicable provisions of these procedures.

(c) (U) If the discrete communication is not to, from, or about a tasked selector but is to or from an identifiable U.S. person, or a person reasonably believed to be located in the United States, the NSA analyst will document that determination in the relevant analytic repository or tool if technically possible or reasonably feasible. Such discrete communication cannot be used for any purpose other than to protect against an immediate threat to human life (e.g., force protection or hostage situations). NSA will report any such use to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which will promptly notify the Foreign Intelligence Surveillance Court of such use.

3. ~~(TS//SI//NF)~~ An NSA analyst seeking to use a discrete communication within an Internet transaction that contains multiple discrete communications in a FISA application, intelligence report, or section 702 targeting must appropriately document the verifications required by subsections 3(b)(4)b.1. and 2. above.

4. ~~(TS//SI//NF)~~ Notwithstanding subsection 3(b)(4)b. above, NSA may use metadata extracted from Internet transactions acquired on or after October 31, 2011, that are not identified and segregated pursuant to subsection 3(b)(4)a. without first assessing whether the metadata was extracted from: a) a discrete communication as to which the sender and all intended recipients are located in the United States; or b) a discrete communication to, from, or about a tasked selector. Any metadata extracted from Internet transactions that are not identified and segregated pursuant to subsection 3(b)(4)a. above will be handled in accordance with the applicable provisions of these procedures. Any metadata extracted from an Internet transaction subsequently determined to contain a discrete communication as to which the sender and all intended recipients are reasonably believed to be located inside the United States shall be destroyed upon recognition.

(5) (U) Magnetic tapes or other storage media containing communications acquired pursuant to section 702 may be scanned by computer to identify and select communications for analysis. Computer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, will be limited to those selection terms reasonably likely to return foreign intelligence information. Identifiers of an identifiable U.S. person may not be used as terms to identify and select for analysis any Internet communication acquired through NSA's upstream

collection techniques. Any use of United States person identifiers as terms to identify and select communications must first be approved in accordance with NSA procedures. NSA will maintain records of all United States person identifiers approved for use as selection terms. The Department of Justice's National Security Division and the Office of the Director of National Intelligence will conduct oversight of NSA's activities with respect to United States persons that are conducted pursuant to this paragraph.

(6) (U) Further handling, retention, and dissemination of foreign communications will be made in accordance with Sections 4, 6, 7, and 8 as applicable, below. Further handling, storage, and dissemination of inadvertently acquired domestic communications will be made in accordance with Sections 4, 5, and 8 below.

(c) (U) Destruction of Raw Data

(1) ~~(S//SI~~ [redacted] Telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers that do not meet the retention standards set forth in these procedures and that are known to contain communications of or concerning United States persons will be destroyed upon recognition. Telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers may not be retained longer than five years from the expiration date of the certification authorizing the collection unless NSA specifically determines that each such communication meets the retention standards in these procedures.

(2) ~~(TS//SI//NF)~~ Internet transactions acquired through NSA's upstream collection techniques that do not contain any information that meets the retention standards set forth in these procedures and that are known to contain communications of or concerning United States persons will be destroyed upon recognition. An Internet transaction may not be retained longer than two years from the expiration date of the certification authorizing the collection unless NSA specifically determines that at least one discrete communication within the Internet transaction meets the retention standards in these procedures and that each discrete communication within the transaction either: (a) is to, from, or about a tasked selector; or (b) is not to, from, or about a tasked selector and is also not to or from an identifiable United States person or person reasonably believed to be in the United States. The Internet transactions that may be retained include those that were acquired because of limitations on NSA's ability to filter communications. Any Internet communications acquired through NSA's upstream collection techniques that are retained in accordance with this subsection may be reviewed and handled only in accordance with the standards set forth above in subsection 3(b)(4) of these procedures.

(3) ~~(TS//SI//NF)~~ Any Internet transactions acquired through NSA's upstream collection techniques prior to October 31, 2011, will be destroyed upon recognition.

(4) ~~(S//NF)~~ NSA may temporarily retain specific section 702-acquired information that would otherwise have to be destroyed, pursuant to section 3(a)-(c) above, if the Department of Justice advises NSA in writing that such information is subject to a preservation obligation in pending or anticipated administrative, civil, or criminal litigation. The specific information to be retained (including, but not limited to, the target(s) or selector(s) whose unminimized information must be preserved and the relevant time period at issue in the litigation), and the particular litigation for which the information will be retained, shall be identified in writing by the Department of Justice. Personnel not working on the particular litigation matter shall not access the unminimized section 702-acquired information preserved pursuant to a written preservation notice from the Department of Justice that would otherwise have been destroyed pursuant to these procedures. Other personnel shall only access the information being retained for litigation-related reasons on a case-by-case basis after consultation with the Department of Justice. The Department of Justice shall notify NSA in writing once the section 702-acquired information is no longer required to be preserved for such litigation matters, and then NSA shall promptly destroy the section 702-acquired information as otherwise required by these procedures. Circumstances could arise requiring that section 702-acquired information subject to other destruction/age off requirements in these procedures (e.g., Section 5) be retained because it is subject to a preservation requirement. In such cases the Government will notify the Foreign Intelligence Surveillance Court and seek permission to retain the material as appropriate consistent with law. Depending on the nature, scope and complexity of a particular preservation obligation, in certain circumstances it may be technically infeasible to retain certain section 702-acquired information. Should such circumstances arise, they will be brought to the attention of the court with jurisdiction over the underlying litigation matter for resolution.

(d) (U) Change in Target's Location or Status

(1) (U//~~FOUO~~) In the event that NSA reasonably believes that a target is located outside the United States and subsequently learns that the person is inside the United States, or if NSA concludes that a target who at the time of targeting was believed to be a non-United States person is in fact a United States person at the time of acquisition, the acquisition from that person will be terminated without delay.

(2) (U) Any communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be located outside the United States but is in fact located inside the United States at the time such communications were acquired, and any communications acquired by targeting a person who at the time of targeting was believed to be a non-United States person but was in fact a United States person at the time such communications were acquired, will be treated as domestic communications under these procedures.

(e) ~~(S//NF)~~ In the event that NSA seeks to use any information acquired pursuant to section 702 during a time period when there is uncertainty about the location of the target of the acquisition because the [redacted] post-tasking checks described in NSA's section 702

targeting procedures were not functioning properly, NSA will follow its internal procedures for determining whether such information may be used (including, but not limited to, in FISA applications, section 702 targeting, and disseminations). Except as necessary to assess location under this provision, NSA may not use or disclose any information acquired pursuant to section 702 during such time period unless NSA determines, based on the totality of the circumstances, that the target is reasonably believed to have been located outside the United States at the time the information was acquired. If NSA determines that the target is reasonably believed to have been located inside the United States at the time the information was acquired, such information will not be used and will be promptly destroyed.

(U) Section 4 - Acquisition and Handling - Attorney-Client Communications

(U) As soon as it becomes apparent that a communication is between a person who is known to be under criminal indictment in the United States and an attorney who represents that individual in the matter under indictment (or someone acting on behalf of the attorney), monitoring of that communication will cease and the communication will be identified as an attorney-client communication in a log maintained for that purpose. The relevant portion of the communication containing that conversation will be segregated and the National Security Division of the Department of Justice will be notified so that appropriate procedures may be established to protect such communications from review or use in any criminal prosecution, while preserving foreign intelligence information contained therein. Additionally, all proposed dissemination of information constituting United States person attorney-client privileged communications must be reviewed by the NSA Office of General Counsel prior to dissemination.

(U) Section 5 - Domestic Communications

~~(TS//SI//NF)~~ A communication identified as a domestic communication (and, if applicable, the Internet transaction in which it is contained) will be promptly destroyed upon recognition unless the Director (or Acting Director) of NSA specifically determines, in writing and on a communication-by-communication basis, that the sender or intended recipient of the domestic communication had been properly targeted under section 702 of the Act, and the domestic communication satisfies one or more of the following conditions:

(1) ~~(TS//SI//NF)~~ such domestic communication is reasonably believed to contain significant foreign intelligence information. Such domestic communication (and, if applicable, the transaction in which it is contained) may be retained, handled, and disseminated in accordance with these procedures;

(2) ~~(TS//SI//NF)~~ such domestic communication does not contain foreign intelligence information but is reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed. Such domestic communication may be disseminated (including United States person identities) to appropriate Federal law enforcement authorities, in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures

set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document. Such domestic communication (and, if applicable, the transaction in which it is contained) may be retained by NSA for a reasonable period of time, not to exceed six months unless extended in writing by the Attorney General, to permit law enforcement agencies to determine whether access to original recordings of such communication is required for law enforcement purposes;

(3) ~~(TS//SI//NF)~~ such domestic communication is reasonably believed to contain technical data base information, as defined in Section 2(j), or information necessary to understand or assess a communications security vulnerability. Such domestic communication may be provided to the FBI and/or disseminated to other elements of the United States Government. Such domestic communication (and, if applicable, the transaction in which it is contained) may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that is, or is reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation.

a. (U//~~FOUO~~) In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis.

b. ~~(S//SI~~ [redacted] In the case of communications that are not enciphered or otherwise reasonably believed to contain secret meaning, sufficient duration is five years from expiration date of the certification authorizing the collection for telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers, and two years from expiration date of the certification authorizing the collection for Internet transactions acquired through NSA's upstream collection techniques, unless the Signal Intelligence Director, NSA, determines in writing that retention of a specific communication for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements; or

(4) (U//~~FOUO~~) such domestic communication contains information pertaining to an imminent threat of serious harm to life or property. Such information may be retained and disseminated to the extent reasonably necessary to counter such threat.

~~(S//NF)~~ Notwithstanding the above, if a domestic communication indicates that a target has entered the United States, NSA may promptly notify the FBI of that fact, as well as any information concerning the target's location that is contained in the communication. NSA may also use information derived from domestic communications for collection avoidance purposes, and may provide such information to the FBI and CIA for collection avoidance purposes. NSA may retain the communication from which such information is

derived but shall restrict the further use or dissemination of the communication by placing it on the Master Purge List (MPL).

(U) Section 6 - Foreign Communications of or Concerning United States Persons

(a) (U) Retention

(U) Foreign communications of or concerning United States persons collected in the course of an acquisition authorized under section 702 of the Act may be retained only:

(1) (U) if necessary for the maintenance of technical data bases. Retention for this purpose is permitted for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation.

a. (U) In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis.

b. ~~(TS//SI//NF)~~ In the case of communications that are not enciphered or otherwise reasonably believed to contain secret meaning, sufficient duration is five years from expiration date of the certification authorizing the collection for telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers, and two years from expiration date of the certification authorizing the collection for Internet transactions acquired through NSA's upstream collection techniques, unless the Signals Intelligence Director, NSA, determines in writing that retention of a specific category of communications for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements;

(2) (U) if dissemination of such communications with reference to such United States persons would be permitted under subsection (b) below; or

(3) (U) if the information is evidence of a crime that has been, is being, or is about to be committed and is provided to appropriate federal law enforcement authorities.

~~(TS//SI//NF)~~ Foreign communications of or concerning United States persons that may be retained under subsections 6(a)(2) and (3) above include discrete communications contained in Internet transactions, provided that NSA has specifically determined, consistent with subsection 3(c)(2) above, that each discrete communication within the Internet transaction either: (a) is to, from, or about a tasked selector; or (b) is not to, from, or about a tasked selector and is also not to or from an identifiable United States person or person reasonably believed to be in the United States.

(b) (U) Dissemination

(U) A dissemination based on communications of or concerning a United States person may be made in accordance with Section 7 or 8 below if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person. Otherwise, dissemination of intelligence based on communications of or concerning a United States person may only be made to a recipient requiring the identity of such person for the performance of official duties but only if at least one of the following criteria is also met:

(1) (U) the United States person has consented to dissemination or the information of or concerning the United States person is available publicly;

(2) (U) the identity of the United States person is necessary to understand foreign intelligence information or assess its importance, e.g., the identity of a senior official in the Executive Branch;

(3) (U) the communication or information indicates that the United States person may be:

a. an agent of a foreign power;

b. a foreign power as defined in section 101(a) of the Act;

c. residing outside the United States and holding an official position in the government or military forces of a foreign power;

d. a corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or

e. acting in collaboration with an intelligence or security service of a foreign power and the United States person has, or has had, access to classified national security information or material;

(4) (U) the communication or information indicates that the United States person may be the target of intelligence activities of a foreign power;

(5) (U) the communication or information indicates that the United States person is engaged in the unauthorized disclosure of classified national security information or the United States person's identity is necessary to understand or assess a communications or network security vulnerability, but only after the agency that originated the information certifies that it is properly classified;

(6) (U) the communication or information indicates that the United States person may be engaging in international terrorist activities;

(7) (U//~~FOUO~~) the acquisition of the United States person's communication was authorized by a court order issued pursuant to the Act and the communication may relate to the foreign intelligence purpose of the surveillance; or

(8) (U) the communication or information is reasonably believed to contain evidence that a crime has been, is being, or is about to be committed, provided that dissemination is for law enforcement purposes and is made in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document.

(c) (U) Provision of Unminimized Communications to CIA and FBI

(1) (U) NSA may provide to the Central Intelligence Agency (CIA) unminimized communications acquired pursuant to section 702 of the Act. CIA will identify to NSA targets for which NSA may provide unminimized communications to CIA. CIA will handle any such unminimized communications received from NSA in accordance with CIA minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act.

(2) (U) NSA may provide to the FBI unminimized communications acquired pursuant to section 702 of the Act. The FBI will identify to NSA targets for which NSA may provide unminimized communications to the FBI. The FBI will handle any such unminimized communications received from NSA in accordance with FBI minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act.

(U) Section 7 - Other Foreign Communications

(U) Foreign communications of or concerning a non-United States person may be retained, used, and disseminated in any form in accordance with other applicable law, regulation, and policy.

(~~TS//SI//NF~~) Foreign communications of or concerning a non-United States person that may be retained under this subsection include discrete communications contained in Internet transactions, provided that NSA has specifically determined, consistent with subsection 3(c)(2) above, that each discrete communication within the Internet transaction either: (a) is to, from, or about a tasked selector; or (b) is not to, from, or about a tasked selector and is also not to or from an identifiable United States person or person reasonably believed to be in the United States.

(U//~~FOUO~~) Additionally, foreign communications of or concerning a non-United States person may be retained for the same purposes and in the same manner as detailed in Section 6(a)(1), above.

(U) Section 8 - Collaboration with Foreign Governments

(a) (U) Procedures for the dissemination of evaluated and minimized information. Pursuant to section 1.7(c)(8) of Executive Order No. 12333, as amended, NSA conducts foreign cryptologic liaison relationships with certain foreign governments. Information acquired pursuant to section 702 of the Act may be disseminated to a foreign government. Except as provided below in subsection 8(b) of these procedures, any dissemination to a foreign government of information of or concerning a United States person that is acquired pursuant to section 702 may only be done in a manner consistent with sections 6(b) and 7 of these NSA minimization procedures.

(b) (U) Procedures for technical or linguistic assistance. It is anticipated that NSA may obtain information or communications that, because of their technical or linguistic content, may require further analysis by foreign governments to assist NSA in determining their meaning or significance. Notwithstanding other provisions of these minimization procedures, NSA may disseminate computer disks, tape recordings, transcripts, or other information or items containing unminimized information or communications acquired pursuant to section 702 to foreign governments for further processing and analysis, under the following restrictions with respect to any materials so disseminated:

(1) (U) Dissemination to foreign governments will be solely for translation or analysis of such information or communications, and assisting foreign governments will make no use of any information or any communication of or concerning any person except to provide technical and linguistic assistance to NSA.

(2) (U) Dissemination will be only to those personnel within foreign governments involved in the translation or analysis of such information or communications. The number of such personnel will be restricted to the extent feasible. There will be no dissemination within foreign governments of this unminimized data.

(3) (U) Foreign governments will make no permanent agency record of information or communications of or concerning any person referred to or recorded on computer disks, tape recordings, transcripts, or other items disseminated by NSA to foreign governments, provided that foreign governments may maintain such temporary records as are necessary to enable them to assist NSA with the translation or analysis of such information. Records maintained by foreign governments for this purpose may not be disseminated within the foreign governments, except to personnel involved in providing technical or linguistic assistance to NSA.

(4) (U) Upon the conclusion of such technical or linguistic assistance to NSA, computer disks, tape recordings, transcripts, or other items or information disseminated to foreign governments will either be returned to NSA or be destroyed with an accounting of such destruction made to NSA.

(5) (U) Any information that foreign governments provide to NSA as a result of such technical or linguistic assistance may be disseminated by NSA in accordance with these minimization procedures.

7/24/14
Date

Eric H. Holder, Jr.
Attorney General of the United States

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

Plaintiff's Exhibit 27

The Guardian



XKeyscore: NSA tool collects 'nearly everything a user does on the internet'

. XKeyscore gives 'widest-reaching' collection of online data . NSA analysts require no prior authorization for searches . Sweeps up emails, social media activity and browsing history . NSA's XKeyscore program – read one of the presentations

Glenn Greenwald

Wed 31 Jul 2013 08.56 EDT

A top secret National Security Agency program allows analysts to search with no prior authorization through vast databases containing emails, online chats and the browsing histories of millions of individuals, according to documents provided by whistleblower Edward Snowden.

The NSA boasts in training materials that the program, called XKeyscore, is its "widest-reaching" system for developing intelligence from the internet.

The latest revelations will add to the intense public and congressional debate around the extent of NSA surveillance programs. They come as senior intelligence officials testify to the Senate judiciary committee on Wednesday, releasing classified documents in response to the Guardian's earlier stories on bulk collection of phone records and Fisa surveillance court oversight.

The files shed light on one of Snowden's most controversial statements, made in his first video interview published by the Guardian on June 10.

"I, sitting at my desk," said Snowden, could "wiretap anyone, from you or your accountant, to a federal judge or even the president, if I had a personal email".

US officials vehemently denied this specific claim. Mike Rogers, the Republican chairman of the House intelligence committee, said of Snowden's assertion: "He's lying. It's impossible for him to do what he was saying he could do."

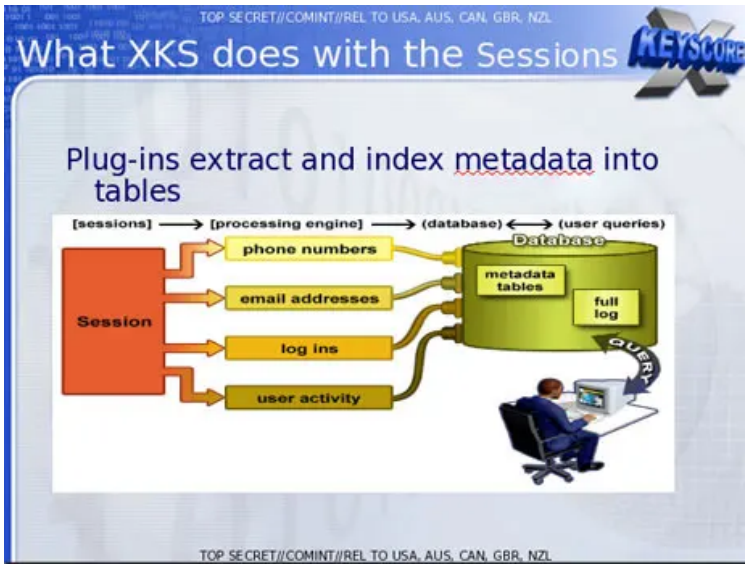
But training materials for XKeyscore detail how analysts can use it and other systems to mine enormous agency databases by filling in a simple on-screen form giving only a broad justification for the search. The request is not reviewed by a court or any NSA personnel before it is processed.

XKeyscore, the documents boast, is the NSA's "widest reaching" system developing intelligence from computer networks - what the agency calls Digital Network Intelligence (DNI). One presentation claims the program covers "nearly everything a typical user does on the internet", including the content of emails, websites visited and searches, as well as their metadata.

Analysts can also use XKeyscore and other NSA systems to obtain ongoing "real-time" interception of an individual's internet activity.

Under US law, the NSA is required to obtain an individualized Fisa warrant only if the target of their surveillance is a 'US person', though no such warrant is required for intercepting the communications of Americans with foreign targets. But XKeyscore provides the technological capability, if not the legal authority, to target even US persons for extensive electronic surveillance without a warrant provided that some identifying information, such as their email or IP address, is known to the analyst.

One training slide illustrates the digital activity constantly being collected by XKeyscore and the analyst's ability to query the databases at any time.



KS1 Photograph: Guardian

The purpose of XKeyscore is to allow analysts to search the metadata as well as the content of emails and other internet activity, such as browser history, even when there is no known email

account (a "selector" in NSA parlance) associated with the individual being targeted.

Analysts can also search by name, telephone number, IP address, keywords, the language in which the internet activity was conducted or the type of browser used.

One document notes that this is because "strong selection [search by email address] itself gives us only a very limited capability" because "a large amount of time spent on the web is performing actions that are anonymous."

The NSA documents assert that by 2008, 300 terrorists had been captured using intelligence from XKeyscore.

Analysts are warned that searching the full database for content will yield too many results to sift through. Instead they are advised to use the metadata also stored in the databases to narrow down what to review.

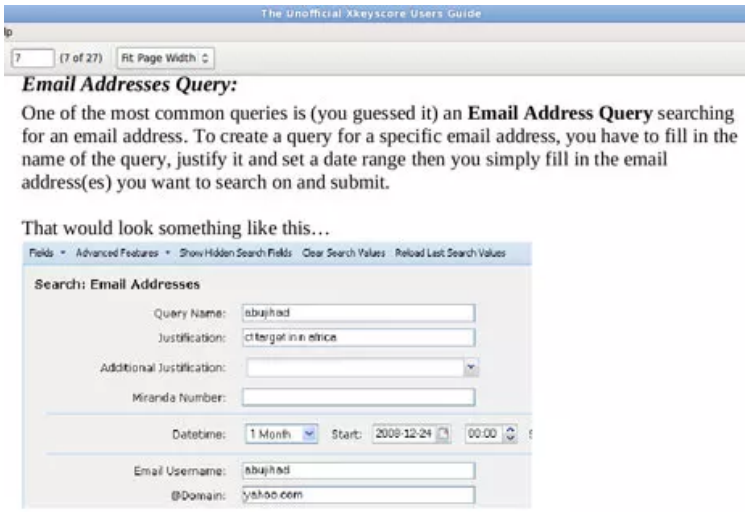
A slide entitled "plug-ins" in a December 2012 document describes the various fields of information that can be searched. It includes "every email address seen in a session by both username and domain", "every phone number seen in a session (eg address book entries or signature block)" and user activity – "the webmail and chat activity to include username, buddylist, machine specific cookies etc".

Email monitoring

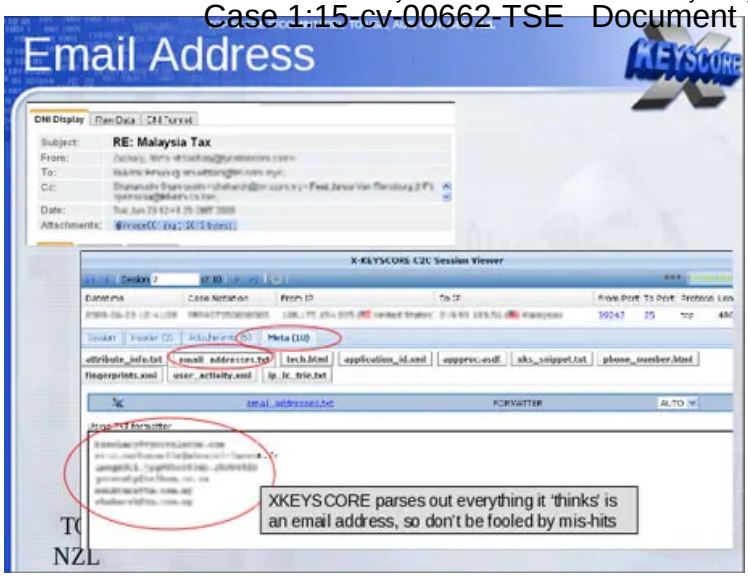
In a second Guardian interview in June, Snowden elaborated on his statement about being able to read any individual's email if he had their email address. He said the claim was based in part on the email search capabilities of XKeyscore, which Snowden says he was authorized to use while working as a Booz Allen contractor for the NSA.

One top-secret document describes how the program "searches within bodies of emails, webpages and documents", including the "To, From, CC, BCC lines" and the 'Contact Us' pages on websites".

To search for emails, an analyst using XKS enters the individual's email address into a simple online search form, along with the "justification" for the search and the time period for which the emails are sought.



KS2 Photograph: Guardian

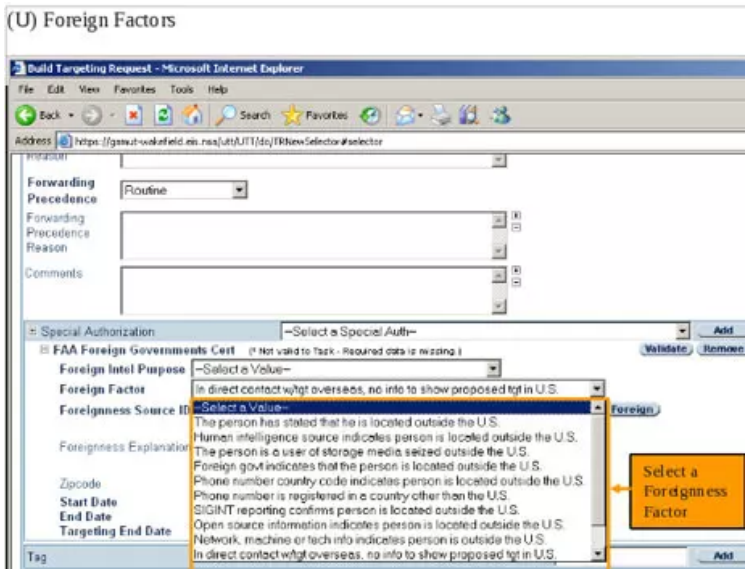


KS3edit2 Photograph: Guardian

The analyst then selects which of those returned emails they want to read by opening them in NSA reading software.

The system is similar to the way in which NSA analysts generally can intercept the communications of anyone they select, including, as one NSA document put it, "communications that transit the United States and communications that terminate in the United States".

One document, a top secret 2010 guide describing the training received by NSA analysts for general surveillance under the Fisa Amendments Act of 2008, explains that analysts can begin surveillance on anyone by clicking a few simple pull-down menus designed to provide both legal and targeting justifications. Once options on the pull-down menus are selected, their target is marked for electronic surveillance and the analyst is able to review the content of their communications:

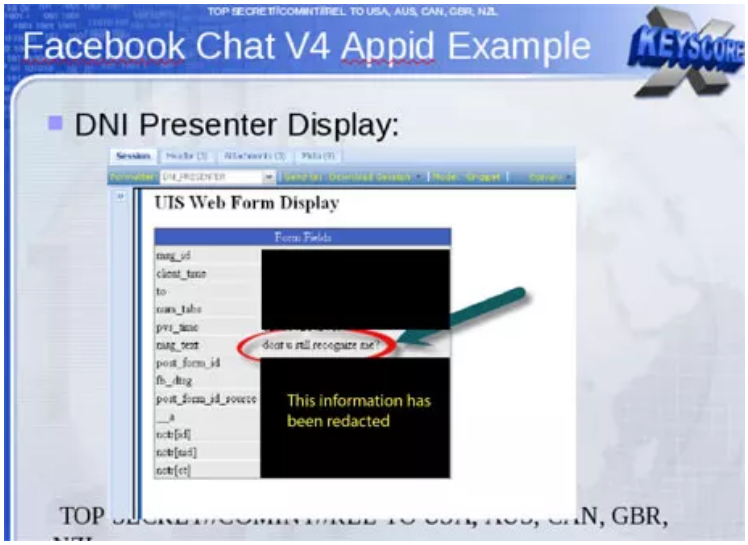


KS4 Photograph: Guardian

Chats, browsing history and other internet activity

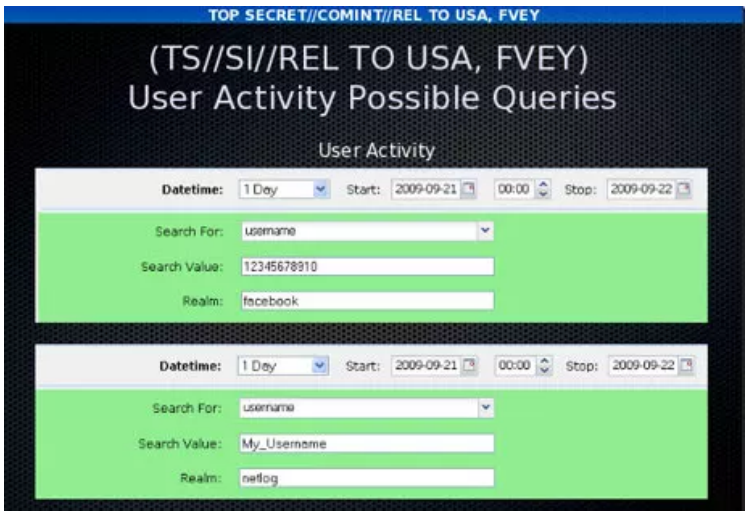
Beyond emails, the XKeyscore system allows analysts to monitor a virtually unlimited array of other internet activities, including those within social media.

An NSA tool called DNI Presenter, used to read the content of stored emails, also enables an analyst using XKeyscore to read the content of Facebook chats or private messages.



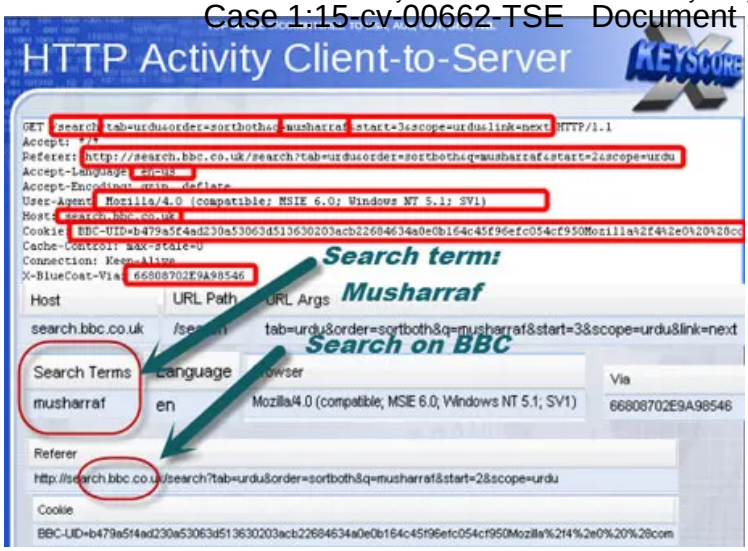
KS55edit Photograph: Guardian

An analyst can monitor such Facebook chats by entering the Facebook user name and a date range into a simple search screen.



KS6 Photograph: Guardian

Analysts can search for internet browsing activities using a wide range of information, including search terms entered by the user or the websites viewed.



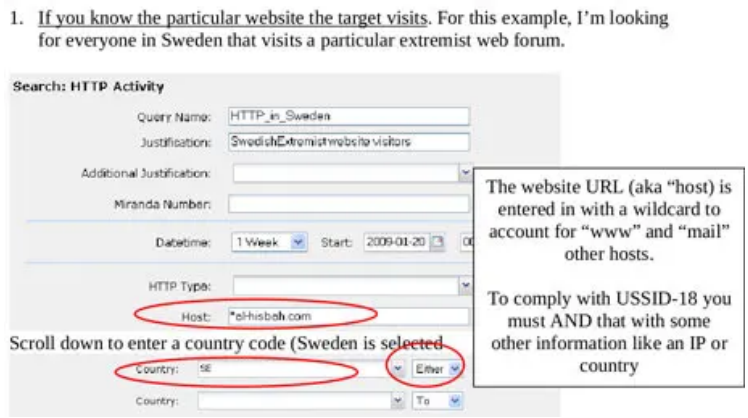
KS7 Photograph: Guardian

As one slide indicates, the ability to search HTTP activity by keyword permits the analyst access to what the NSA calls "nearly everything a typical user does on the internet".



KS8 Photograph: Guardian

The XKeyscore program also allows an analyst to learn the IP addresses of every person who visits any website the analyst specifies.



KS9 Photograph: Guardian

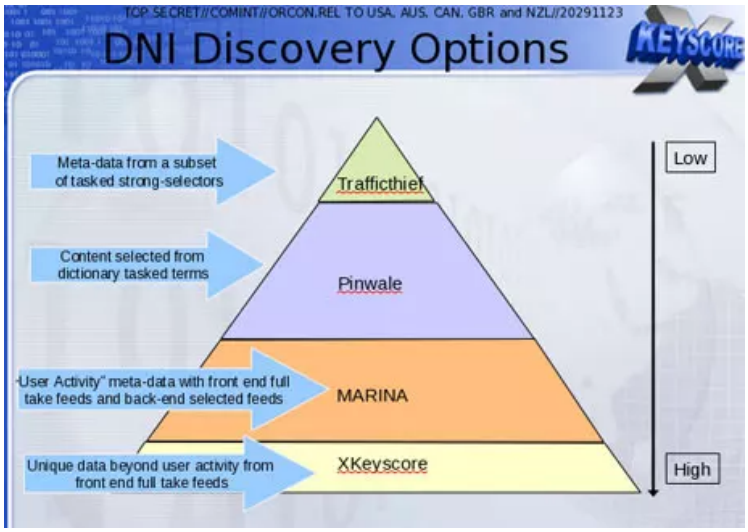
The quantity of communications accessible through programs such as XKeyscore is staggeringly large. One NSA report from 2007 estimated that there were 850bn "call events" collected and stored in the NSA databases, and close to 150bn internet records. Each day, the document says, 1-2bn records were added.

William Binney, a former NSA mathematician, said last year that the agency had "assembled on the order of 20tn transactions about US citizens with other US citizens", an estimate, he said, that "only was involving phone calls and emails". A 2010 Washington Post article reported that "every day, collection systems at the [NSA] intercept and store 1.7bn emails, phone calls and other type of communications."

The XKeyscore system is continuously collecting so much internet data that it can be stored only for short periods of time. Content remains on the system for only three to five days, while metadata is stored for 30 days. One document explains: "At some sites, the amount of data we receive per day (20+ terabytes) can only be stored for as little as 24 hours."

To solve this problem, the NSA has created a multi-tiered system that allows analysts to store "interesting" content in other databases, such as one named Pinwale which can store material for up to five years.

It is the databases of XKeyscore, one document shows, that now contain the greatest amount of communications data collected by the NSA.



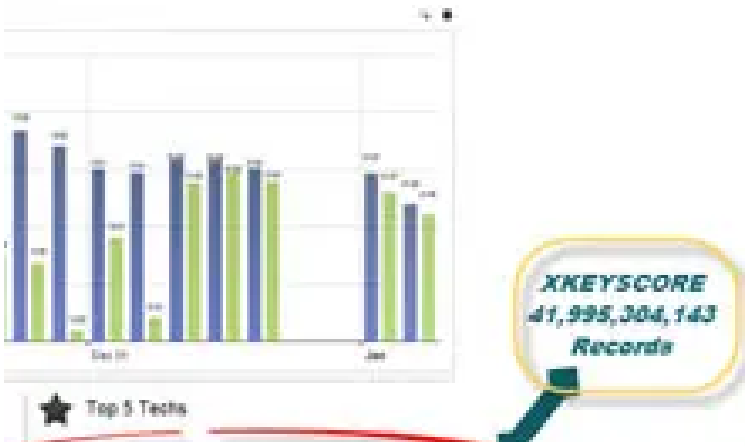
KS10 Photograph: Guaridan

In 2012, there were at least 41 billion total records collected and stored in XKeyscore for a single 30-day period.

Legal v technical restrictions

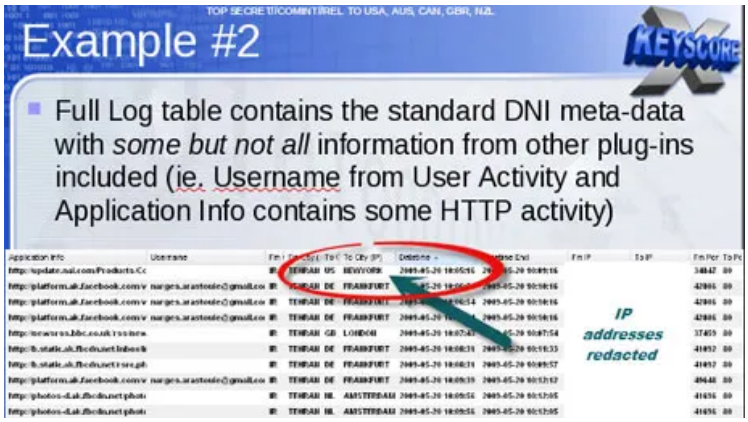
While the Fisa Amendments Act of 2008 requires an individualized warrant for the targeting of US persons, NSA analysts are permitted to intercept the communications of such individuals without a warrant if they are in contact with one of the NSA's foreign targets.

The ACLU's deputy legal director, Jameel Jaffer, told the Guardian last month that national security officials expressly said that a primary purpose of the new law was to enable them to collect large amounts of Americans' communications without individualized warrants.



"The government doesn't need to 'target' Americans in order to collect huge volumes of their communications," said Jaffer. "The government inevitably sweeps up the communications of many Americans" when targeting foreign nationals for surveillance.

An example is provided by one XKeyscore document showing an NSA target in Tehran communicating with people in Frankfurt, Amsterdam and New York.



KS12 Photograph: Guardian

In recent years, the NSA has attempted to segregate exclusively domestic US communications in separate databases. But even NSA documents acknowledge that such efforts are imperfect, as even purely domestic communications can travel on foreign systems, and NSA tools are sometimes unable to identify the national origins of communications.

Moreover, all communications between Americans and someone on foreign soil are included in the same databases as foreign-to-foreign communications, making them readily searchable without warrants.

Some searches conducted by NSA analysts are periodically reviewed by their supervisors within the NSA. "It's very rare to be questioned on our searches," Snowden told the Guardian in June, "and even when we are, it's usually along the lines of: 'let's bulk up the justification'."

In a letter this week to senator Ron Wyden, director of national intelligence James Clapper acknowledged that NSA analysts have exceeded even legal limits as interpreted by the NSA in domestic surveillance.

Acknowledging what he called "a number of compliance problems", Clapper attributed them to "human error" or "highly sophisticated technology issues" rather than "bad faith".

However, Wyden said on the Senate floor on Tuesday: "These violations are more serious than those stated by the intelligence community, and are troubling."

In a statement to the Guardian, the NSA said: "NSA's activities are focused and specifically deployed against - and only against - legitimate foreign intelligence targets in response to requirements that our leaders need for information necessary to protect our nation and its interests.

"XKeyscore is used as a part of NSA's lawful foreign signals intelligence collection system.

"Allegations of widespread, unchecked analyst access to NSA collection data are simply not true. Access to XKeyscore, as well as all of NSA's analytic tools, is limited to only those personnel who require access for their assigned tasks ... In addition, there are multiple technical, manual and supervisory checks and balances within the system to prevent deliberate misuse from occurring."

"Every search by an NSA analyst is fully auditable, to ensure that they are proper and within the law.

"These types of programs allow us to collect the information that enables us to perform our missions successfully - to defend the nation and to protect US and allied troops abroad."

$0
contributed
$0
our goal

In these critical times ...

... Guardian columnist and author Rebecca Solnit urges you to show your support for independent journalism with a year-end gift to The Guardian. We are asking our US readers to help us raise $1 million dollars by the new year to report on the most important stories in 2019.

A note from Rebecca:

“First they came for the journalists,” said the young man’s sign. “We don’t know what happened after that.” It’s a brilliant comment that underscores two things. One is how utterly necessary it is to a free, powerful, informed public, to have the ability to act on what happens beyond our own horizon, to make choices about our governments whether by blockading a senate or parliament or electing people we’ve learned about from the news.

The other is how much tyrants and would-be tyrants fear a free press - and what your enemies think is often the best way to measure whether you matter. They know autocracy depend on keeping the public ignorant on some fronts and misinformed on others.

We’ve seen direct attacks on journalists in the past year, from the murder of Jamal Khashoggi to Trump’s incessant attacks on the media as “the enemy of the people,” and for a couple of decades we’ve seen the indirect attacks that are Silicon Valley’s siphoning off of advertising revenue and amplification of untruths for profit.

It costs a lot to send someone out to cover a campaign or to investigate a crime; it’s hard work that requires expertise and support from our readers. This year, The Guardian has covered everything from tech to feminism to Trump to fossil fuel politics. It is our editorial independence that has

allowed us to deliver this fearless reporting; an independence that's sometimes hard to find in other US-based media. We hope you appreciate our efforts.

We want to say a huge thank you to everyone who has supported The Guardian so far. We hope to pass our goal by early January 2019. Every contribution, big or small, will help us reach it. **Please make a year-end gift today to show your ongoing support for our independent journalism. Thank you.**

Support The Guardian



Topics

- The NSA files
- Glenn Greenwald on security and liberty
- Surveillance
- NSA
- Privacy
- Internet
- Data protection
- US politics
- news

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

Plaintiff's Exhibit 28

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Why are we interested in HTTP?









Because nearly everything a typical user does on the Internet uses HTTP











JA3221

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

Plaintiff's Exhibit 29

The Intercept_

XKEYSCORE

NSA's Google for the World's Private Communications



Morgan Marquis-Boire, Glenn Greenwald, Micah Lee

July 1 2015, 10:49 a.m.

One of the National Security Agency's most powerful tools of mass surveillance makes tracking someone's Internet usage as easy as entering an email address, and provides no built-in technology to prevent abuse. Today, *The Intercept* is publishing 48 top-secret and other classified documents about XKEYSCORE dated up to 2013, which shed new light on the breadth, depth and functionality of this critical spy system — one of the largest releases yet of documents provided by NSA whistleblower Edward Snowden.

The NSA's XKEYSCORE program, first revealed by *The Guardian*, sweeps up countless people's Internet searches, emails, documents, usernames and passwords, and other private communications. XKEYSCORE is fed a constant flow of Internet traffic from fiber optic cables that make up the backbone of the world's communication network, among other sources, for processing. As of 2008, the surveillance system boasted approximately 150 field sites in the United States, Mexico, Brazil, United Kingdom, Spain, Russia, Nigeria, Somalia, Pakistan, Japan, Australia, as well as many other countries, consisting of over 700 servers.

These servers store "full-take data" at the collection sites – meaning that they captured all of the traffic collected – and, as of 2009, stored content for 3 to 5 days and metadata for 30 to 45 days. NSA documents indicate that tens of billions of records are stored in its database. "It is a fully distributed processing and query system that runs on machines around the world," an NSA briefing on XKEYSCORE says. "At field sites, XKEYSCORE can run on multiple computers that gives it the ability to scale in both processing power and storage."

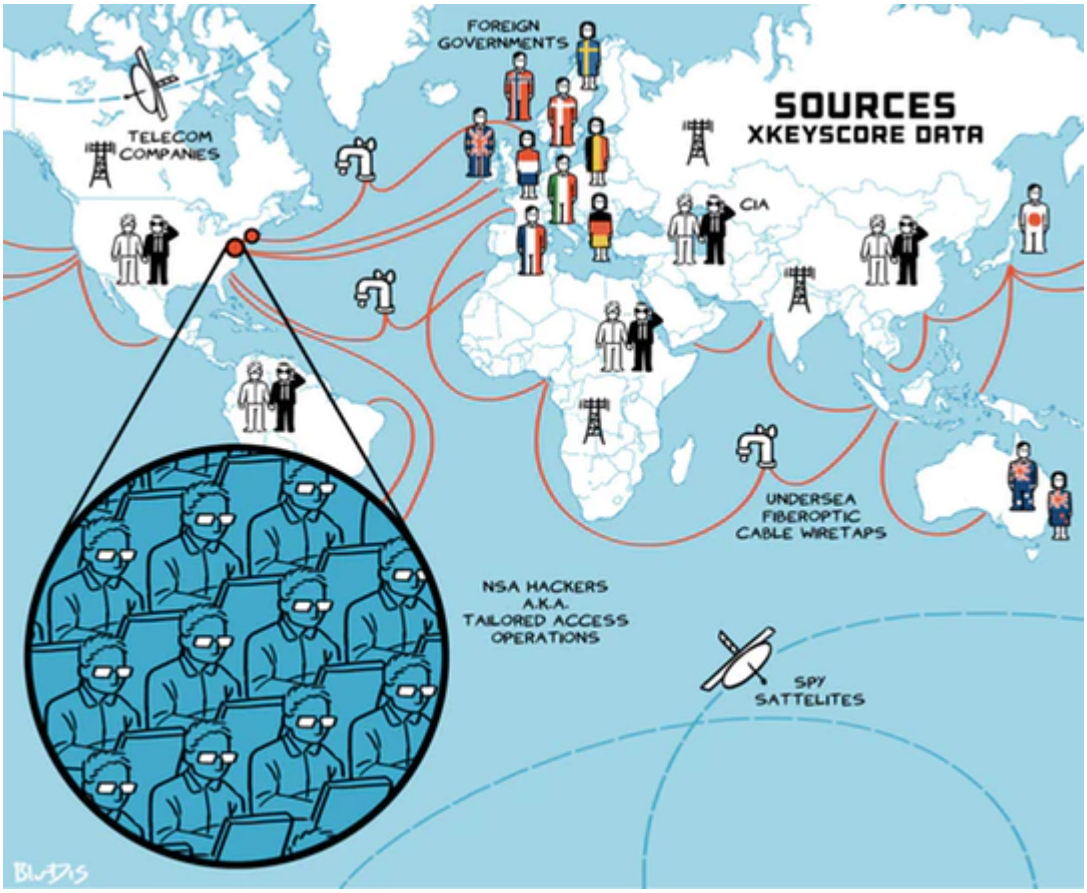


Illustration: Blue Delliquanti and David Axe for The Intercept

XKEYSCORE also collects and processes Internet traffic from Americans, though NSA analysts are taught to avoid querying the system in ways that might result in spying on U.S. data. Experts and privacy activists, however, have long doubted that such exclusions are effective in preventing large amounts of American data from being swept up. One document *The Intercept* is publishing today suggests that FISA warrants

have authorized "full-take" collection of traffic from at least some U.S. web forums.

The system is not limited to collecting web traffic. The 2013 document, "VoIP Configuration and Forwarding Read Me," details how to forward VoIP data from XKEYSCORE into NUCLEON, NSA's repository for voice intercepts, facsimile, video and "pre-released transcription." At the time, it supported more than 8,000 users globally and was made up of 75 servers absorbing 700,000 voice, fax, video and tag files per day.

The reach and potency of XKEYSCORE as a surveillance instrument is astonishing. The *Guardian* report noted that NSA itself refers to the program as its "widest reaching" system. In February of this year, *The Intercept* reported that NSA and GCHQ hacked into the internal network of Gemalto, the world's largest provider of cell phone SIM cards, in order to steal millions of encryption keys used to protect the privacy of cell phone communication. XKEYSCORE played a vital role in the spies' hacking by providing government hackers access to the email accounts of Gemalto employees.

Numerous key NSA partners, including Canada, New Zealand and the U.K., have access to the mass surveillance databases of XKEYSCORE. In March, the *New Zealand Herald*, in partnership with *The Intercept*, revealed that the New Zealand government used XKEYSCORE to spy on candidates for the position of World Trade Organization director general and also members of the Solomon Islands government.

These newly published documents demonstrate that collected communications not only include emails, chats and web-browsing traffic, but also pictures, documents, voice calls, webcam photos, web searches, advertising analytics traffic, social media traffic, botnet traffic, logged keystrokes, computer network exploitation (CNE) targeting, intercepted username and password pairs, file uploads to online services, Skype sessions and more.

Bulk collection and population surveillance

XKEYSCORE allows for incredibly broad surveillance of people based on perceived patterns of suspicious behavior. It is possible, for instance, to query the system to show the activities of people based on their location, nationality and websites visited. For instance, one slide displays the search "germansinpakistn," showing an analyst querying XKEYSCORE for all individuals in Pakistan visiting specific German language message boards.

As sites like Twitter and Facebook become increasingly significant in the world's day-to-day communications (a Pew study shows that 71 percent of online adults in the U.S. use Facebook), they become a critical source of surveillance data. Traffic from popular social media sites is described as "a great starting point" for tracking individuals, according to an XKEYSCORE presentation titled "Tracking Targets on Online Social Networks."

When intelligence agencies collect massive amounts of Internet traffic all over the world, they face the challenge of making sense of that data. The vast quantities collected make it difficult to connect the stored traffic to specific individuals.

Internet companies have also encountered this problem and have solved it by tracking their users with identifiers that are unique to each individual, often in the form of browser cookies. Cookies are small pieces of data that websites store in visitors' browsers. They are used for a variety of purposes, including authenticating users (cookies make it possible to log in to websites), storing preferences, and uniquely tracking individuals even if they're using the same IP address as many other people. Websites also embed code used by third-party services to

collect analytics or host ads, which also use cookies to track users. According to one slide, "Almost all websites have cookies enabled."

The NSA's ability to piggyback off of private companies' tracking of their own users is a vital instrument that allows the agency to trace the data it collects to individual users. It makes no difference if visitors switch to public Wi-Fi networks or connect to VPNs to change their IP addresses: the tracking cookie will follow them around as long as they are using the same web browser and fail to clear their cookies.

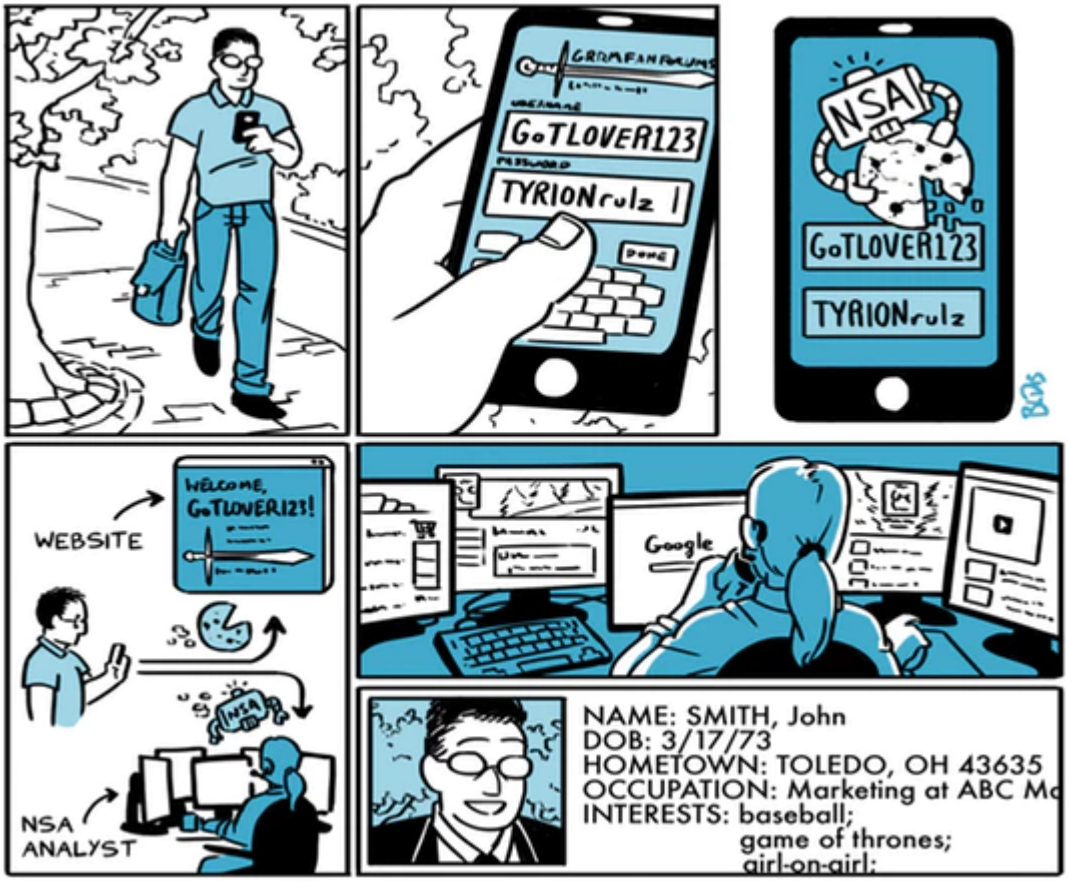


Illustration: Blue Delliquanti and David Axe for The Intercept

Apps that run on tablets and smartphones also use analytics services that uniquely track users. Almost every time a user sees an advertisement (in an app or in a web browser), the ad network is tracking users in the same way. A secret GCHQ and CSE program called BADASS, which is similar to XKEYSCORE but with a much narrower scope, mines as much valuable information from leaky smartphone

apps as possible, including unique tracking identifiers that app developers use to track their own users. In May of this year, CBC, in partnership with *The Intercept*, revealed that XKEYSCORE was used to track smartphone connections to the app marketplaces run by Samsung and Google. Surveillance agency analysts also use other types of traffic data that gets scooped into XKEYSCORE to track people, such as Windows crash reports.

In a statement to *The Intercept*, the NSA reiterated its position that such sweeping surveillance capabilities are needed to fight the War on Terror:

"The U.S. Government calls on its intelligence agencies to protect the United States, its citizens, and its allies from a wide array of serious threats. These threats include terrorist plots from al-Qaeda, ISIL, and others; the proliferation of weapons of mass destruction; foreign aggression against the United States and our allies; and international criminal organizations."

Indeed, one of the specific examples of XKEYSCORE applications given in the documents is spying on Shaykh Atiyatallah, an al Qaeda senior leader and Osama bin Laden confidant. A few years before his death, Atiyatallah did what many people have often done: He googled himself. He searched his various aliases, an associate and the name of his book. As he did so, all of that information was captured by XKEYSCORE.

XKEYSCORE has, however, also been used to spy on non-terrorist targets. The April 18, 2013 issue of the internal NSA publication Special Source Operations Weekly boasts that analysts were successful in using XKEYSCORE to obtain U.N. Secretary General Ban Ki-moon's talking points prior to a meeting with President Obama.

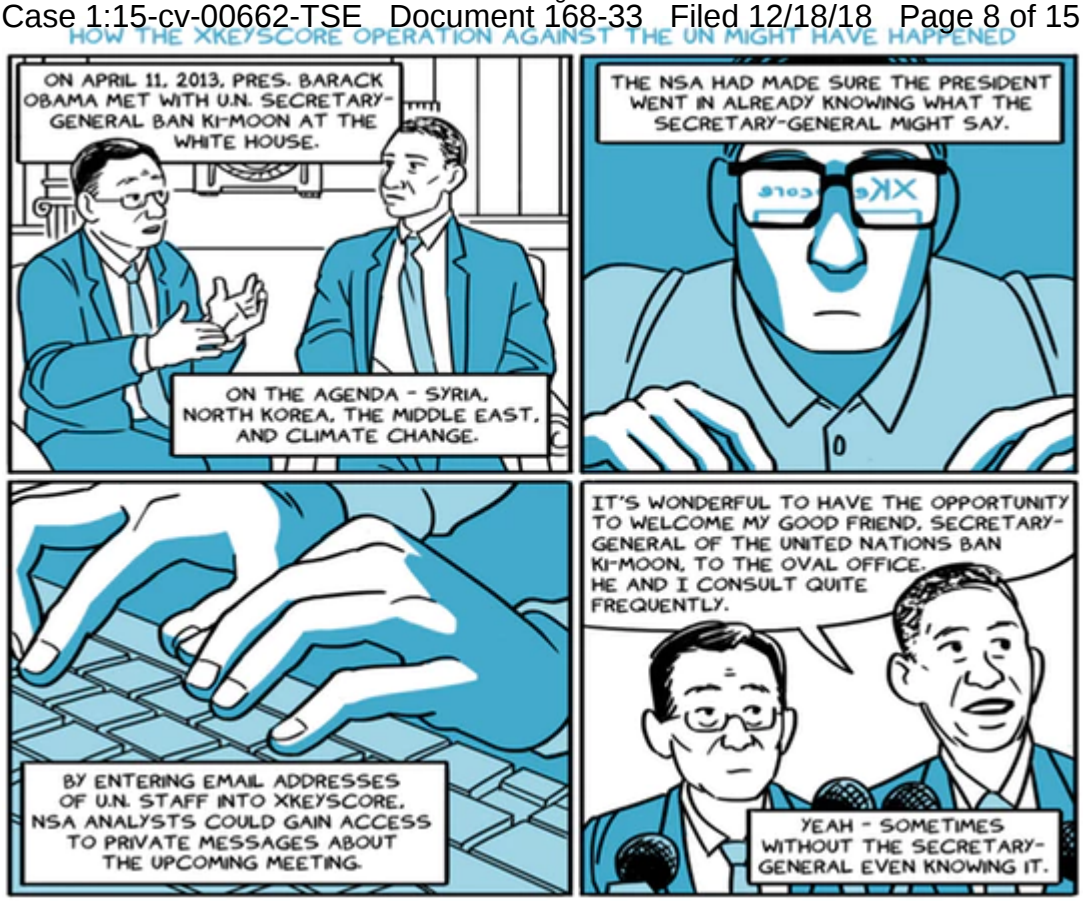


Illustration: Blue Delliquanti and David Axe for The Intercept

XKEYSCORE for hacking: Easily collecting user names, passwords and much more

XKEYSCORE plays a central role in how the U.S. government and its surveillance allies hack computer networks around the world. One top-secret 2009 NSA document describes how the system is used by the NSA to gather information for the Office of Tailored Access Operations, an NSA division responsible for Computer Network Exploitation (CNE) – i.e., targeted hacking.

Particularly in 2009, the hacking tactics enabled by XKEYSCORE would have yielded significant returns as use of encryption was less widespread than today. Jonathan Brossard, a security researcher and the

CEO of Toucan Systems, told *The Intercept*: "Anyone could be trained to do this in less than one day: they simply enter the name of the server they want to hack into XKEYSCORE, type enter, and are presented login and password pairs to connect to this machine. Done. Finito." Previous reporting by *The Intercept* revealed that systems administrators are a popular target of the NSA. "Who better to target than the person that already has the 'keys to the kingdom?'" read a 2012 post on an internal NSA discussion board.

This system enables analysts to access web mail servers with remarkable ease.

The same methods are used to steal the credentials – user names and passwords – of individual users of message boards.

Hacker forums are also monitored for people selling or using exploits and other hacking tools. While the NSA is clearly monitoring to understand the capabilities developed by its adversaries, it is also monitoring locations where such capabilities can be purchased.

Other information gained via XKEYSCORE facilitates the remote exploitation of target computers. By extracting browser fingerprint and operating system versions from Internet traffic, the system allows analysts to quickly assess the exploitability of a target. Brossard, the security researcher, said that "NSA has built an impressively complete set of automated hacking tools for their analysts to use."

Given the breadth of information collected by XKEYSCORE, accessing and exploiting a target's online activity is a matter of a few mouse clicks. Brossard explains: "The amount of work an analyst has to perform to actually break into remote computers over the Internet seems ridiculously reduced – we are talking minutes, if not seconds. Simple. As easy as typing a few words in Google."

These facts bolster one of Snowden's most controversial statements, made in his first video interview published by *The Guardian* on June 9, 2013. "I, sitting at my desk," said Snowden, could "wiretap anyone, from you or your accountant, to a federal judge to even the president, if I had a personal email."

Indeed, training documents for XKEYSCORE repeatedly highlight how user-friendly the program is: with just a few clicks, any analyst with access to it can conduct sweeping searches simply by entering a person's email address, telephone number, name or other identifying data. There is no indication in the documents reviewed that prior approval is needed for specific searches.

In addition to login credentials and other target intelligence, XKEYSCORE collects router configuration information, which it shares with Tailored Access Operations. The office is able to exploit routers and then feed the traffic traveling through those routers into their collection infrastructure. This allows the NSA to spy on traffic from otherwise out-of-reach networks. XKEYSCORE documents reference router configurations, and a document previously published by *Der Spiegel* shows that "active implants" can be used to "cop[y] traffic and direc[t]" it past a passive collector.

XKEYSCORE for counterintelligence

Beyond enabling the collection, categorization, and querying of metadata and content, XKEYSCORE has also been used to monitor the surveillance and hacking actions of foreign nation states and to gather the fruits of their hacking. *The Intercept* previously reported that NSA and its allies spy on hackers in order to collect what they collect.

Once the hacking tools and techniques of a foreign entity (for instance, South Korea) are identified, analysts can then extract the country's espionage targets from XKEYSCORE, and gather information that the foreign power has managed to steal.

Monitoring of foreign state hackers could allow the NSA to gather techniques and tools used by foreign actors, including knowledge of zero-day exploits – software bugs that allow attackers to hack into systems, and that not even the software vendor knows about – and implants. Additionally, by monitoring vulnerability reports sent to vendors such as Kaspersky, the agency could learn when exploits they were actively using need to be retired because they've been discovered by a third party.

Seizure v. searching: Oversight, audit trail and the Fourth Amendment

By the nature of how it sweeps up information, XKEYSCORE gathers communications of Americans, despite the Fourth Amendment protection against "unreasonable search and seizure" – including searching data without a warrant. The NSA says it does not target U.S. citizens' communications without a warrant, but acknowledges that it "incidentally" collects and reads some of it without one, minimizing the information that is retained or shared.

But that interpretation of the law is dubious at best.

XKEYSCORE training documents say that the "burden is on user/auditor to comply with USSID-18 or other rules," apparently including the British Human Rights Act (HRA), which protects the rights of U.K. citizens. U.S. Signals Intelligence Directive 18 (USSID 18) is the American directive that governs "U.S. person minimization."

Kurt Opsahl, the Electronic Frontier Foundation's general counsel, describes USSID 18 as "an attempt by the intelligence community to comply with the Fourth Amendment. But it doesn't come from a court, it comes from the executive."

If, for instance, an analyst searched XKEYSCORE for all iPhone users, this query would violate USSID 18 due to the inevitable American iPhone users that would be grabbed without a warrant, as the NSA's own training materials make clear.

Opsahl believes that analysts are not prevented by technical means from making queries that violate USSID 18. "The document discusses whether auditors will be happy or unhappy. This indicates that compliance will be achieved by after-the-fact auditing, not by preventing the search."

Screenshots of the XKEYSCORE web-based user interface included in slides show that analysts see a prominent warning message: "This system is audited for USSID 18 and Human Rights Act compliance." When analysts log in to the system, they see a more detailed message warning that "an audit trail has been established and will be searched" in response to HRA complaints, and as part of the USSID 18 and USSID 9 audit process.

Because the XKEYSCORE system does not appear to prevent analysts from making queries that would be in violation of these rules, Opsahl concludes that "there's a tremendous amount of power being placed in the hands of analysts." And while those analysts may be subject to audits, "at least in the short term they can still obtain information that they shouldn't have."

During a symposium in January 2015 hosted at Harvard University, Edward Snowden, who spoke via video call, said that NSA analysts are "completely free from any meaningful oversight." Speaking about the

people who audit NSA systems like XKEYSCORE for USSID 18 compliance, he said, "The majority of the people who are doing the auditing are the friends of the analysts. They work in the same office. They're not full-time auditors, they're guys who have other duties assigned. There are a few traveling auditors who go around and look at the things that are out there, but really it's not robust."

In a statement to *The Intercept*, the NSA said:

"The National Security Agency's foreign intelligence operations are 1) authorized by law; 2) subject to multiple layers of stringent internal and external oversight; and 3) conducted in a manner that is designed to protect privacy and civil liberties. As provided for by Presidential Policy Directive 28 (PPD-28), all persons, regardless of their nationality, have legitimate privacy interests in the handling of their personal information. NSA goes to great lengths to narrowly tailor and focus its signals intelligence operations on the collection of communications that are most likely to contain foreign intelligence or counterintelligence information."

Coming next: A Look at the Inner Workings of XKEYSCORE

Source maps: XKS as a SIGDEV Tool, p. 15, and XKS Intro, p. 6

Documents published with this article:

- Advanced HTTP Activity Analysis
- Analyzing Mobile Cellular DNI in XKS
- ASFD Readme
- CADENCE Readme
- Category Throttling
- CNE Analysis in XKS
- Comms Readme

- DEEPDIVE Readme
- DNI101
- Email Address vs User Activity
- Free File Uploaders
- Finding and Querying Document Metadata
- Full Log vs HTTP
- Guide to Using Contexts in XKS Fingerprints
- HTTP Activity in XKS
- HTTP Activity vs User Activity
- Intro to Context Sensitive Scanning With XKS Fingerprints
- Intro to XKS AppIDs and Fingerprints
- OSINT Fusion Project
- Phone Number Extractor
- RWC Updater Readme
- Selection Forwarding Readme
- Stats Config Readme
- Tracking Targets on Online Social Networks
- TRAFFICTHIEF Readme
- Unofficial XKS User Guide
- User Agents
- Using XKS to Enable TAO
- UTT Config Readme
- VOIP in XKS
- VOIP Readme
- Web Forum Exploitation Using XKS
- Writing XKS Fingerprints
- XKS Application IDs
- XKS Application IDs Brief
- XKS as a SIGDEV Tool
- XKS, Cipher Detection, and You!
- XKS for Counter CNE
- XKS Intro

- XKS Logos Embedded in Docs
- XKS Search Forms
- XKS System Administration
- XKS Targets Visiting Specific Websites
- XKS Tech Extractor 2009
- XKS Tech Extractor 2010
- XKS Workflows 2009
- XKS Workflows 2011
- UN Secretary General XKS


We depend on the support of readers like you to help keep our nonprofit newsroom strong and independent. **Join Us →**

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

Plaintiff's Exhibit 30



XKEYSCORE for Counter-CNE

"Using the XKS CNE dataset and a DISGRUNTLEDDUCK fingerprint, we now see at least 21 TAO boxes with evidence of this intrusion set, most of which are associated with projects aimed at Iran WMD targets." **-- MHS, July 2010**

March, 2011

[redacted]

xks-cne@r1.r.nsa

UNCLASSIFIED//FOUO

Overall Classification

The overall classification of this presentation is:

TOP SECRET//COMINT//REL TO USA, FVEY

UNCLASSIFIED//FOUO

What is XKEYSCORE?



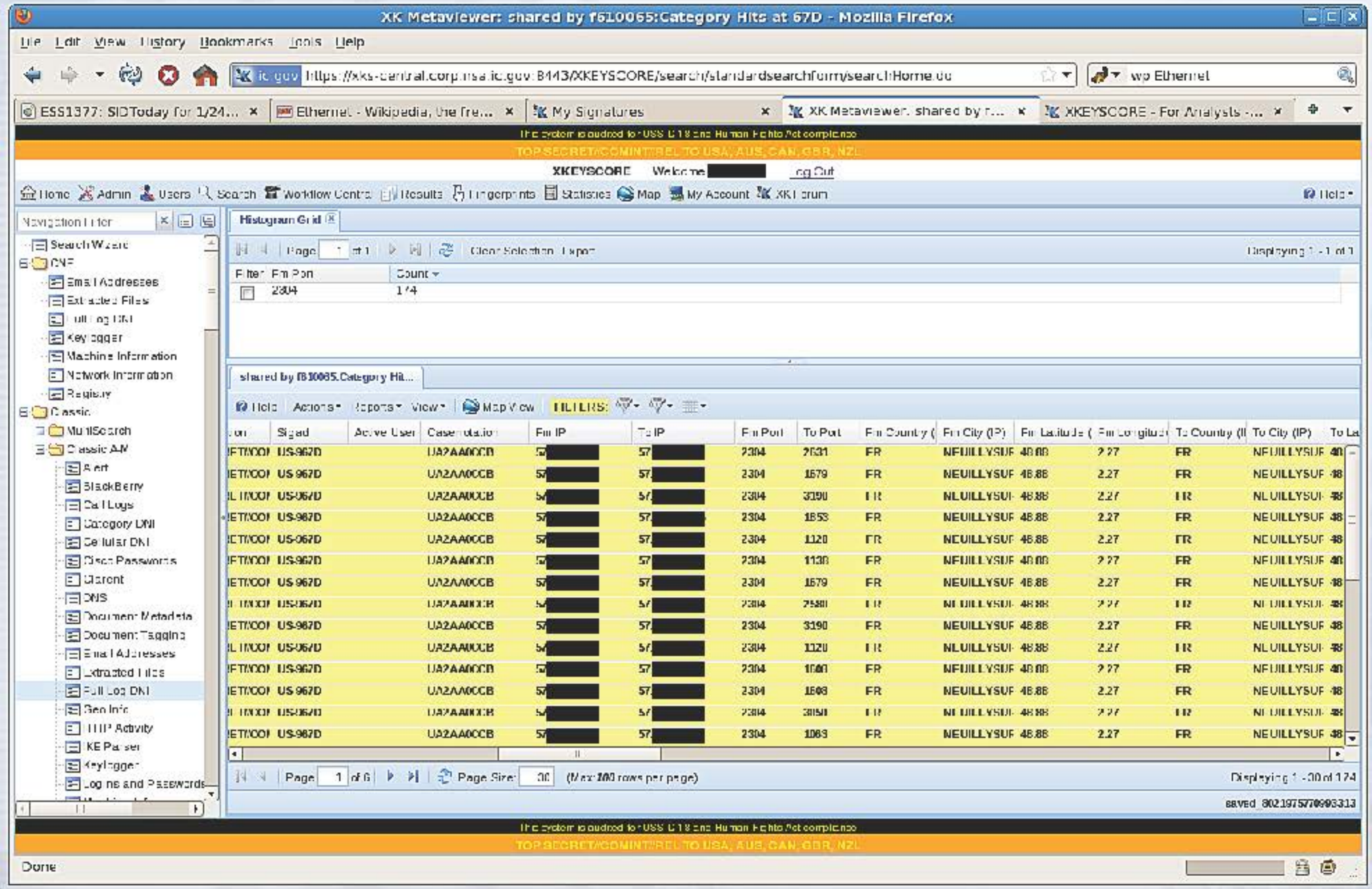
- A suite of software running on a Linux host
- *Classically*, used for DNI processing, selection and survey
- A distributed hierarchy of servers at field sites and headquarters
  - Extract and tag metadata & content from traffic
  - Servicing analyst queries and workflows
- Web and programmatic front-ends

What is XKEYSCORE?



- A suite of software running on a Linux host
- *Classically*, used for DNI processing, selection and survey
- A distributed hierarchy of servers at field sites and headquarters
  - Extract and tag metadata & content from traffic
  - Servicing analyst queries and workflows
- Web and programmatic front-ends

XKEYSCORE GUI



Example Search



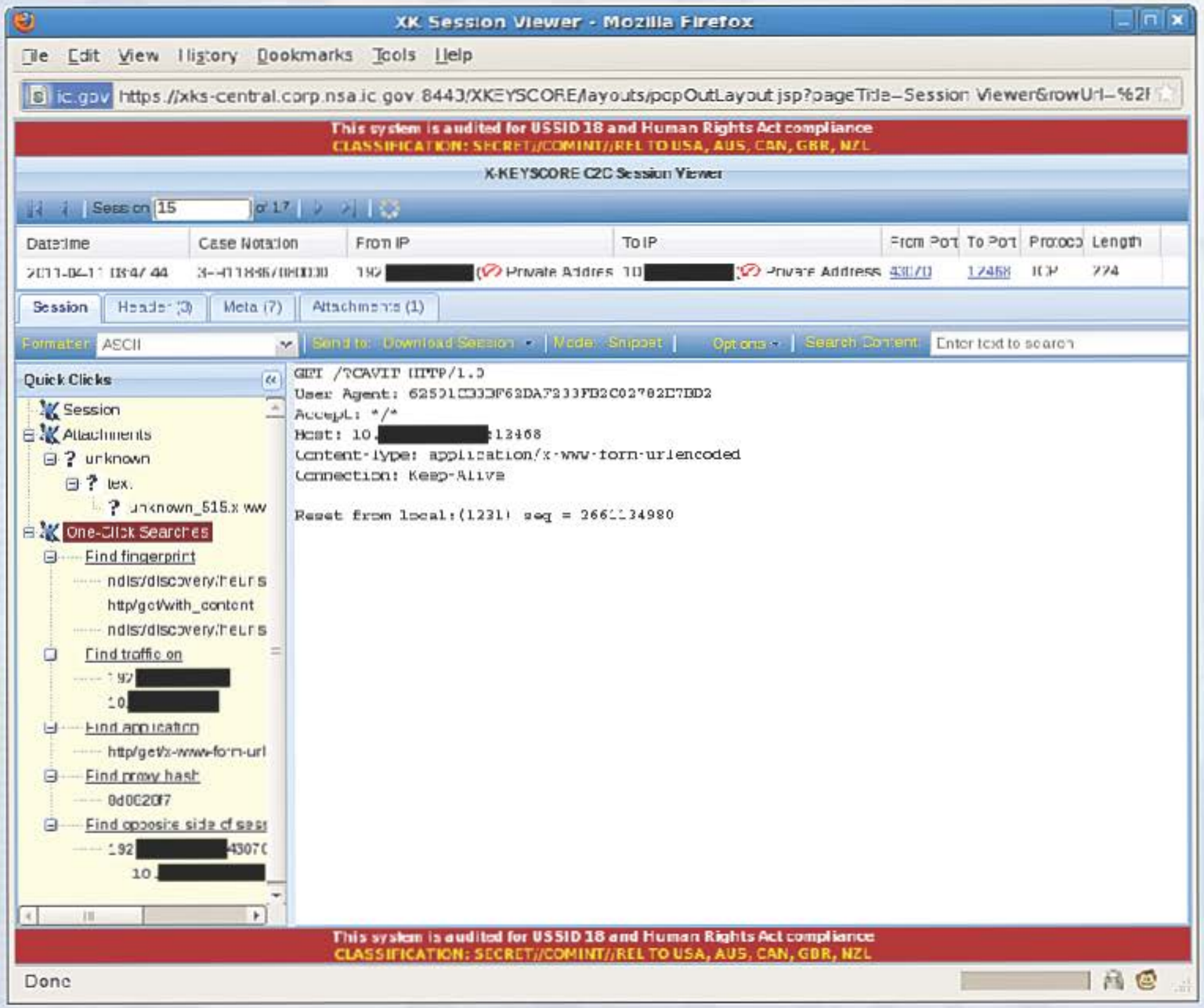
- Let's try a search for suspicious stuff...

  http_activity search, 5-eyes defeat, look for fingerprints:

  `ndist/discovery/heuristic/BHAM/get_with_content` or `http/get/with_content`

- While the search runs, some gotchas:
  - You choose where your query is run
  - Content and metadata age-off
  - Burden is on user/auditor to comply with USSID-18 or other rules
  - Geolocation based on IP

Search Results



Notes:

- Strange User-Agent
- Probably NOT CNE but definitely something non-standard
- Content: maybe a HTTP tunnel for some weird protocol?

  `Reset from local...`
- Should we write a Fingerprint?

Fingerprints and Appids



- Useful for identifying classes of traffic or particular targets (for SIGDEV or collection):

  `mail/webmail/yahoo`

  `browser/cellphone/blackberry`

  `topic/s2B/chinese_missile`

- appid – a contest, highest scoring appid wins
- fingerprint – many fingerprints per session
- microplugin – a fingerprint or appid that is relatively complex (e.g. extracts and databases metadata)

SECRET//COMINT//REL TO USA, FVEY

Fingerprints and Appids (more)



- Written in language called "GENESIS" (go genesis-language):

```
appid('encyclopedia/wikipedia', 2.0) =
   http_host('wikipedia' or 'wikimedia');
fingerprint('dns/malware/MalwareDomains') =
   dns_host(' erofreex.info ' or ' datayakoz.info '
   or ' erogirlx.info ' or ' pornero.info ' or ...
```

- If a fingerprint contains a `schema` definition, a search form automatically appears in the XKEYSCORE GUI
- Power users can drop in to C++ to express themselves

SECRET//COMINT//REL TO USA, FVEY

More about searches



- Many different searches
  - Base search is **Full Log DNI**
  - Depending on traffic type, will generate searchable results for (example):

HTTP Activity	Network Information	GEO Info
Extracted Files	Email Addresses	Registry
Logins and Passwords	Document Metadata	Machine Info

- workflow – a user query that is run automatically usually every 24 hours

XKEYSCORE Gotchas

- Not all sites run latest XKEYSCORE software or fingerprints
- fingerprint submission:
  - XKEYSCORE team weighs mission-worthiness of user fingerprints vs computational cost
- Content and metadata ageoff

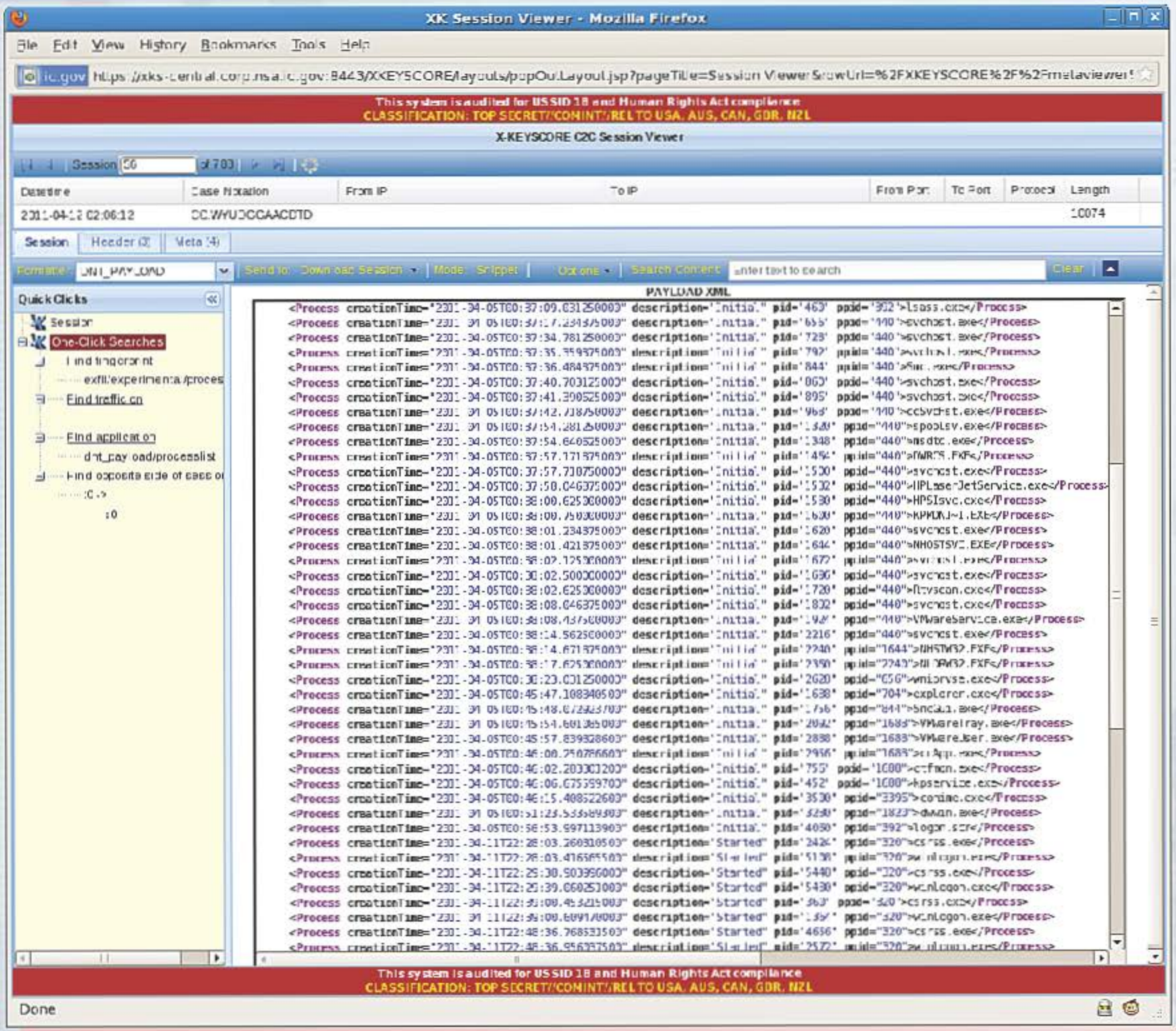
XKEYSCORE CNE

- Lots of endpoint data flows into XKS
  TAO (no ECIs), GCHQ (almost all)
- Other limited flows include SIGINT Forensics Center, TAO STAT
- XKEYSCORE works well for endpoint data
- Sometimes the paradigm breaks (e.g. collected browser history file)

XKEYSCORE CNE (more)

- Payload types:
  `dirwalk, extracted file, system survey, network config, captured credentials, registry query, key logger, etc.`
- Labeled `dnt_payload` in appid/fingerprint ontology
- Let's look at some DANDERSPRITZ data...

XKEYSCORE CNE (more)



XKEYSCORE CNE (more)

- Recent Developments
  - Upgrade of XKEYSCORE CNE
  - Keyloggers: keylogger/perfect/extension
  - PCAP Reingestion
- Router Redirection

Counter CNE Methodology

(refer to Counter CNE Resources slide...)

- Hypothesis/research-driven
  - "Could South Korean CNE be using similar selectors to FVEY CNE?"
  - "What keywords could be used to find keyloggers ("example: keylog OR keystroke")
- Bogus or Unusual Traffic
  - HTTP GET with content (example in this presentation)
  - HTTP POST at odd hours (from Russia 0200-0359Z)
  - Funky user agents
- Known-Host or User driven (e.g. drop sites)
- XKEYSCORE is GOOD at these kinds of things

CNE-Specific

- Registry searches (e.g. SIMBAR)
- Fused Active/Passive search
  - common selectors
  - document hashes
- Known Processes (malicious executables or code)

  ... Let's enhance the process list appid
- map-reduce within CNE cluster using GENESIS calls

XKEYSCORE Doesn't Do...

- ... at all (well, automatically, anyways)
  - Paired traffic heuristic-based approach
    - HTTP[S] imbalance (e.g. GET without response)
    - IP/DNS mismatch*
- ... on an automatic basis
  - Network or host characterization
  - Changes in IP/DNS mapping over time
  - Changes over time in malware comms

Counter CNE Resources



- *How to Discover Intrusions [using XKEYSCORE]* by [redacted] and [redacted] (paper)
- MHS INDEX – Foreign CNE Discovery Page
  https://wiki.itd.nsa/wiki/Foreign_CNE_Discovery
- CSEC and GCHQ – DONUT (unknown protocols):
  https://tiso.sigint.cse/snipehunt/index.php/DONUT
- GCHQ Discovery Posted some Research of Detecting Man-on-the-Side Attacks:
  https://tiso.sigint.cse/snipehunt/index.php/MOTS

GCQH Disco Team posts POC's for different Intrusions and some Details:
https://wiki.gchq/index.php/Discovery

- The GCHQ DISCO team also posts Discovery Theories they run once a week:
  https://wiki.gchq/index.php/Discovery_Afternoons
- XKEYSCORE Fingerprints

Success Story – MHS INDEX

KEYSCORE

Using TAO-obtained Iranian implant encryption keys, inline decrypt using XKS microplugin – IRGC-QF keylogger data!

XK Session Viewer - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://xks-central.corp.nsa.ic.gov:8443/XKEYSCORE/layouts/popOutLayout.jsp?pageTitle=Session Viewer&rowUrl=%2FXKEYSCORE%2F%2Fmetaview

This system is audited for USSID 18 and Human Rights Act compliance
CLASSIFICATION: TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

X-KEYSCORE C2C Session Viewer

Session 15 of 70

Datetime	Case Notation	From IP	To IP	From Por	To Port	Protoc	Length
2011-03-28 19:51:28	IRS1014	78.[redacted] (Iran)	174.[redacted] (United States)	42325	80	tcp	3203

Session | Header (3) | Attachments (2) | Meta (9)

Formatter: AUTO | Send to: Download Session | Mode: Snippet | Options | Search Content: Enter text to search

Quick Clicks

- Session
- Attachments
  - unknown
    - text
      - keylogger.txt
      - unknown_1931.x-www-
- One-Click Searches
  - Find fingerprint
    - ntoc/ntocg/malware/amulets
    - botnet/AMULETSTELLAR/k
  - Find traffic on
    - 78.38.110.163
    - 174.132.180.34
  - Find application
    - mail/webmail/yahoo
  - Find proxy hash
    - c8b0d875
  - Find opposite side of session
    - 78.[redacted]:42325 ->
      174.[redacted]:

Download this from XKEYSCORE

keylogger.txt | FORMATTER | AUTO

Virus scan results | Clean

Using TXT formatter

```
<< (2 unread) Yahoo! Mail, mehrab.raisi - Mozilla Firefox >>

[] [] [] [
```

Points of Contact

- MHS Index Team
  - [redacted]: [redacted]@nsa.ic.gov
- CES/TRANGRESSION
  - [redacted]: [redacted]@nsa.ic.gov
  - [redacted]: [redacted]@nsa.ic.gov
- NSA/Countering Foreign Intelligence
  - [redacted]: [redacted]@nsa.ic.gov
- NTOC ??
- XKEYSCORE
  - [redacted], [redacted]: xks-cne@r1.r.nsa

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

Plaintiff's Exhibit 31

WIKIMEDIA META-WIKI

Main page
Wikimedia News
Translations
Recent changes
Random page
Help
Babel

Community

Wikimedia Resource Center
Wikimedia Forum
Mailing lists
Requests
Babylon
Reports
Research
Planet Wikimedia

Beyond the Web

Meet Wikimedians
Events
Movement affiliates
Donate

Print/export

Create a book
Download as PDF
Printable version

Tools

What links here
Related changes
Special pages
Permanent link
Page information
Cite this page
Link by ID

In other languages

Add links

Founding principles

Translate this page; This page contains changes which are not marked for translation.

Other languages:	العربية • مصرى • asturianu • беларуская (тарашкевіца) • български • català • čeština • Cymraeg • dansk • Deutsch • Zazaki • Ελληνικά • **English** • Esperanto • español • euskara • فارسی • français • • magyar • Bahasa Indonesia • italiano • 日本語 • • 한국어 • Lëtzebuergesch • Baso Minangkabau • • Bahasa Melayu • Nederlands • occitan • polski • پښتو • português • português do Brasil • русский • سنڌي • slovenčina • slovenščina • Basa Sunda • svenska • • • • ไทย • Türkçe • татарча/tatarça • українська • 中文

Wikimedia projects have certain **founding principles** in common. These principles may evolve or be refined over time, but they are considered ideals essential to the founding of the Wikimedia projects – not to be confused with the Wikimedia Foundation (which also arose from the Wikimedia projects). People who strongly disagree with them are nonetheless expected to either respect them while collaborating on the site or turn to another site. Those unable or unwilling sometimes end up leaving the project.

These principles include:

1. Neutral point of view (NPOV) as a guiding editorial principle.
2. The ability of almost anyone to edit (most) articles without registration.
3. The "wiki process" as the final decision-making mechanism for all content.
4. The creation of a welcoming and collegial editorial environment.
5. Free licensing of content; in practice defined by each project as public domain, GFDL, CC BY-SA or CC BY.
6. Maintaining room for fiat to help resolve particularly difficult problems. On a dozen projects, an Arbitration Committee has the authority to make certain binding, final decisions such as banning an editor.

Variants [edit]

Not all projects follow these principles in the same way.

- Some apply neutrality by allowing a plurality of items which are individually not neutral (Commons, which says "Commons is not Wikipedia, and files uploaded here do not necessarily need to comply with the Neutral point of view"), or have a simpler principle of 'being fair' (Wikivoyage, which says "Travel guides should *not* be written from a neutral point of view").
- Some allow non-wiki modes of collaboration and decision-making in some parts of their process (MediaWiki).
- Some allow limited use of fair-use media or other media that are not freely licensed.

See also [edit]

- Wikimedia Foundation mission statement
- Wikimedia values — The six values of the Wikimedia Foundation
- In a nutshell, what is Wikipedia? And what is the Wikimedia Foundation? — The Wikimedia Foundation

Categories: Community | Global policies

This page was last edited on 27 February 2018, at 07:58.

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. See Terms of Use for details.

Privacy policy About Meta Disclaimers Developers Cookie statement Mobile view

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

Plaintiff's Exhibit 32

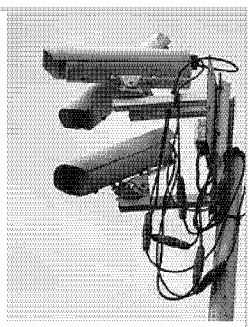
COMMUNITY, GLOBAL, LEGAL, WIKIMEDIA

Opposing Mass Surveillance on the Internet

By Yana Welinder
May 9th, 2014

Surveillance cameras, Quevaal, CC BY-SA 3.0. We are pleased to announce that the Wikimedia Foundation is signing the Necessary and Proportionate Principles on the application of human rights to surveillance. Privacy on the Internet is closely connected to our mission to disseminate free knowledge.[1] 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

We are pleased to announce that the Wikimedia Foundation is signing the Necessary and Proportionate Principles on the application of human rights to surveillance.



Surveillance cameras, Quevaal, CC BY-SA 3.0.

Privacy on the Internet is closely connected to our mission to disseminate free knowledge.[1] 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.

Although the recent conversation about internet surveillance was spurred by the revelation of a US government program, PRISM, a report issued by the United Nations Special Rapporteur on the Freedom of Opinion and Expression makes it clear that surveillance by governments is global, ubiquitous, and generally unchecked. The Necessary and Proportionate Principles are intended to provide a framework for human rights laws to address modern surveillance technologies.[2] They demand that governments respect international law and human rights by complying with basic principles such as:

- **Proportionality**: Surveillance of communications is highly intrusive and implicates privacy rights and freedom of expression. This should be carefully weighed against any benefit sought to be achieved.
- **User Notification**: Individuals need to know if they will be the subject of surveillance and have enough time and information to appeal the decision.
- **Transparency**: Countries must be transparent about the extent of surveillance and the techniques employed.

GET CONNECTED

GET OUR EMAIL UPDATES

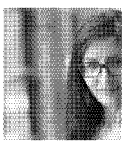
Your email address

Subscribe

MEET OUR COMMUNITY



The one-man band writing the history of Nigerian cinema into Wikipedia



Wikipedia is a to "plant and harvest" free knowledge: Ar Aghayan

More Community Profiles

MOST VIEWED THIS MONTH

'Monumental' winners from th world's largest photo contest showcase history and heritage

The top fifteen images from Wiki...

Türkiye'den Vikipedi'ye erişim engeli halen devam ediyor

Vikipedi'nin tüm dil sürümleri, Nisan ayını

New monthly dataset shows w people fall into Wikipedia rabl holes

The Wikimedia Foundation's Analytics te

ARCHIVES

FEBRUARY 2018

JANUARY 2018

- **Integrity of Communications and Systems**: Governments should not compel ISPs or hardware and software vendors to build monitoring capability into their systems.

The Necessary and Proportionate Principles project was led by several groups, including the Electronic Frontier Foundation, Access, and Privacy International. The principles were developed through a consultation with civil society groups and international experts in communications surveillance law, policy, and technology. So far, the Principles have been advocated by over 400 organizations and many individuals. The signatories include Wikimedia Mexico and several Wikimedians. Today, we are proud to join their efforts.

Yana Welinder
Legal Counsel, Wikimedia Foundation[3]

1. ↑ As we previously discussed, the Foundation believes that government surveillance can compromise our values of freedom of speech and access to information.
2. ↑ For more information about the purpose of the Principles, see here.
3. ↑ Special thanks to Roshni Patel, WMF Privacy Fellow, for her work on this blog post.

DECEMBER 2017
NOVEMBER 2017
OCTOBER 2017
OLDER POSTS 26

WORK AT WIKIMEDIA

Work with the foundation that supports W and its sister projects around the world. A and join us

5 Comments on Opposing Mass Surveillance on the Internet

Global Ceo 3 years

The people are massivelly supporting the uncencored internet and the founder of internet agrees with them. http://globalceo.com/tim-berners-lee-web-should-be-basis-of-democracy/

Share

Fae 4 years

Sorry, the links embedded in my last post do not seem to have been included. These were:
1. An email "Use of this list as evidence of consultation" to the Advocacy Advisors list
http://lists.wikimedia.org/pipermail/advocacy_advisors/2014-May/thread.html
2. The discussion in 2013 by Wikimedia UK volunteers at
https://wikimedia.org.uk/wiki/Water_cooler/2013#International_Principles_on_the_Application_of_Human_Rights_to_Communications_Surveillance

Share

Fae 4 years

Hi Roshni, thanks for your prompt response.

I was not aware of the Advocacy Advisors email list, members of that list are neither elected nor are Wikimedia groups such as Wikimedia LGBT asked to provide representation on the list. It is not evidence of community consultation. I have today joined the list and raised this question of scope at .

Your personal reading of the document does not agree with mine, or many other Wikimedians, the discussion in 2013 by Wikimedia UK volunteers at may be a helpful reference.

The list under "Legitimate Aim" uses wording that cannot be assumed to be defined by the preamble. Further, it is clear that in any country where LGBT activities were unlawful, any legally recognized organization would have no obligation to respect the private lives of LGBT minorities. The document appears to deliberately circumvent this issue by its careful choice of wording. As a relatively short set of principles, where other minority groups have been specifically listed for protection, yet LGBT or sexual orientation remains invisible, can only be a political convenience so that the principles do not break the law in countries where homosexuality is unlawful.

I am deeply disappointed that the community was not widely consulted so that this problem could not be properly discussed, before committing the Foundation to this flawed document.

Share

Roshni Patel 4 years

Hi Fae,

Prior to signing on to the Necessary and Proportionate Principles, we consulted the advocacy advisors. You can find that here.

The list of prohibited discriminations under the "Legitimate Aim" principle is non-exclusive and includes "other status." Given that sexual orientation was listed in the preamble, it would certainly be included under "other status".

Share

Fae 4 years

The document will be offensive to many, as LGBT minorities have been explicitly excluded from the "Legitimate Aim" section, despite "sexual orientation" being mentioned in the unenforceable preamble. As a consequence this policy supports any Government who wish to track LGBT minorities for any reason. In the light of countries recently attempting to make having a profile on Grindr a crime for its citizens, this is not a theoretical scenario.

Could someone please provide some links to the necessary community consultation in advance of this political action of the WMF?

Share

Comments are closed.

WIKIMEDIA FOUNDATION
The Wikimedia Foundation, Inc is a nonprofit charitable organization dedicated to encouraging the growth, development and distribution of free, multilingual content, and to providing the full content of these wiki-based projects to the public free of charge. Get Involved | Log In

WIKIMEDIA PROJECTS

The Wikimedia Foundation operates some of the largest collaboratively edited reference projects in the world.

WIKIPEDIA COMMONS MEDIAWIKI WIKIBOOKS
WIKIDATA WIKINEWS WIKIQUOTE WIKISOURCE
WIKISPECIES WIKIVERSITY WIKIVOYAGE WIKTIONARY

WIKIMEDIA MOVEMENT AFFILIATES

The Wikimedia projects have an international scope, and the Wikimedia movement ha already made a significant impact throughout the world. To continue this success on a organizational level, Wikimedia is building an international network of associated organizations.

WIKIMEDIA CHAPTERS THEMATIC ORGANIZATIONS WIKIMEDIA USER GROUPS

This work is licensed under a Creative Commons Attribution 3.0 unported license. Some images under CC BY-SA.
Read our Terms of Use and Privacy policy. | Powered by WordPress.com VIP

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

Plaintiff's Exhibit 33

Wikimedia Public Policy

Policy Action List

email address JOIN

Join our mailing list to keep up with our policy initiatives.

Privacy

Everyone should be free to read and write without governments looking over their shoulders.



"What Are You Looking At?" by Jonas Bengtsson, licensed under CC BY 2.0 / cropped.

Why You Should Care

- Privacy is essential for our intellectual freedom: reading, writing, and researching.
- People should be free to read and write without fear of governments or advertisers looking over their shoulder.
- Privacy can be an important personal preference even for those that have nothing to hide.

Privacy is the bedrock of intellectual freedom and thus of free knowledge. It sustains freedom of expression and association, which in turn enable inquiry, dialogue, and creation. Privacy is essential to Wikimedia's vision of empowering everyone to share in the sum of all human knowledge. People should not have to look over their shoulders before searching, pause before contributing to controversial articles, or refrain from sharing verifiable but unpopular information.

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.

People also need to feel comfortable that they can read Wikipedia without the fear that the government or other third parties are tracking or watching them. Therefore, all traffic to and from the Wikimedia projects is encrypted through the HTTPS protocol. We also use Strict Transport Security (HSTS), which instructs web browsers to only interact with Wikimedia projects over an encrypted connection, protecting against efforts to break HTTPS and intercept traffic.

Your Help is Welcome

To discuss or help translate this page visit the public policy discussion group.

Wikimedia projects are not built in isolation. The privacy practices of other sites with reliable sources impact the Wikimedia mission to collect and share knowledge. For our free knowledge projects to work, we need security and privacy across the internet so editors and readers can freely research the sources needed to build Wikipedia.

In particular, internet users cannot be subjected to mass surveillance, which chills intellectual curiosity and creativity. Privacy is a fundamental right recognised under international law like the International Covenant on Civil and Political Rights (Article 17) and the Universal Declaration of Human Rights (Article 12). Indiscriminate mass surveillance violates this fundamental right. We strongly oppose mass surveillance by any government or entity. To that end, we signed the Necessary and Proportionate Principles on the application of human rights to surveillance that demand that governments respect basic principles such as:

- Proportionality: The need for surveillance should be carefully weighed against the implications for privacy rights and freedom of expression.
- User Notification: Individuals who will be the subject of surveillance must have enough time and information to appeal the decision.

- Transparency: Governments must be transparent about the extent of surveillance and the techniques they employ.
- Integrity of communication and systems: Governments should not compel internet service providers of hardware and software vendors to build monitoring capability into their systems.

In a time when the collection of private data has become a business model, Wikimedians believe in the importance of privacy. This human right protects our users and consequently the creation of free knowledge.

Related Resources

Global surveillance disclosures (2013–present)

Privacy by Design

Necessary and Proportionate

To discuss or help translate this page visit the public policy discussion group.

Keep up-to-date with Wikimedia's policy initiatives

email address JOIN

The list admins will not give your email address to others.

Wikimedia Public Policy

Learn more about the Wikimedia Foundation.

Privacy Policy | *About*

Our Topics

Access

Copyright

Censorship

Intermediary Liability

Privacy

Wikipedia® and other Wikimedia project names and logos are registered trademarks of the Wikimedia Foundation, a non-profit organization.

USCA4 Appeal: 20-1191 Doc: 18-5 Filed: 07/01/2020 Pg: 395 of 529

Text licensed under Creative Commons Attribution-ShareAlike 3.0 unported. Images are freely licensed with attribution.

Powered by WordPress.com VIP

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

Plaintiff's Exhibit 34

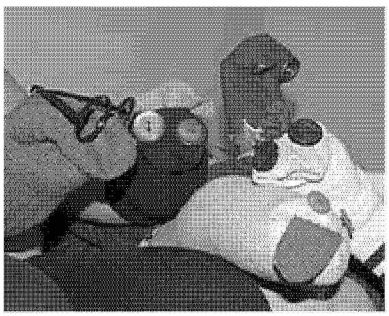
WIKIPEDIA

Wikipedia:Sock puppetry

This page documents an English Wikipedia policy.
It describes a widely accepted standard that all editors should normally follow. Changes made to it should reflect consensus.

This page in a nutshell: The general rule is **one editor, one account**. Do not use multiple accounts to mislead, deceive, vandalize or disrupt; to create the illusion of greater support for a position; to stir up controversy; or to circumvent a block, ban, or sanction. Do not ask your friends to create accounts to support you. Do not revive old unused accounts and use them as different users, or use another person's account. Do not log out just to vandalize as an IP address editor.

Editors are generally expected to edit using at most one account. This improves accountability and increases community trust. While there are some valid reasons for maintaining multiple accounts, improper uses of multiple accounts (called **sock puppetry**, or **socking**) include attempts to deceive or mislead other editors, disrupt discussions, distort consensus, avoid sanctions, evade blocks, or otherwise violate community standards and policies.


The origin of the term "sock puppet" is a type of toy puppet.

Sock puppetry takes various forms:

- Logging out to make problematic edits as an IP address
- Creating new accounts to avoid detection
- Using another person's account (piggybacking)
- Reviving old unused accounts (sometimes referred to as *sleepers*) and presenting them as different users
- Persuading friends or colleagues to create accounts for the purpose of supporting one side of a dispute (usually called meatpuppetry)

Misuse of multiple accounts is a serious breach of community trust. It may lead to:

- a block of all affected accounts
- a ban of the user (the *sockmaster* or *sockpuppeteer*) behind the accounts (each of which is a *sockpuppet* or *sock*)
- on-project exposure of all accounts and IP addresses used across Wikipedia and its sister projects
- the (potential) public exposure of any "real-world" activities or personal information deemed relevant to preventing future sock puppetry or certain other abuses.[1]

Conduct policies

Aspersions
Block evasion
Civility
Clean start
Consensus
Dispute resolution
Edit warring
Editing policy
Harassment
Non-discrimination policy
No personal attacks

USCA4 Appeal: 20-1191 Doc: 18-5 Filed: 07/01/2020 Pg: 398 of 529

Ownership of content

Sock puppetry

Username policy

Vandalism

An editor using multiple accounts for *valid* reasons should, on each account's user page, list all the other accounts with an explanation of their purpose (see below). Optionally, the user and user talk pages of some of the accounts can be redirected to those of another. Editors who use unlinked alternative accounts, or who edit as an IP address editor separate from their account, should carefully avoid any crossover on articles or topics because even innocuous activities such as copy editing, wikifying, or linking might be considered sock puppetry in some cases and innocuous intentions will not usually serve as an excuse.

Contents

Inappropriate uses of alternative accounts

Legitimate uses
- Editing while logged out

Alternative account notification

Meatpuppetry
- Sharing an IP address

Handling suspected sock puppets
- Sockpuppet investigations
- CheckUser
- Blocking
- Tagging

Proving you are not a sock

List of role accounts

See also
- Guidelines
- Essays

References

External links

Inappropriate uses of alternative accounts

Editors must not use alternative accounts to mislead, deceive, disrupt, or undermine consensus. This includes, but is not limited to:

- **Creating an illusion of support**: Alternative accounts must not be used to give the impression of more support for a position than actually exists.
- **Editing project space**: Undisclosed alternative accounts are not to be used in discussions internal to the project.[2]

- **Circumventing policies**: Policies apply per person, not per account. Policies such as the three-revert rule are for each person's edits. Using a second account to violate policy will cause any penalties to be applied to your main account.
- **Strawman socks**: Creating a separate account to argue one side of an issue in a deliberately irrational or offensive fashion, to sway opinion to another side.
- **Evasion of sanctions**: Sanctions apply to individual editors, not to accounts. Using a second account to edit in violation of an active block or community sanction will result in further sanctions, which may include removal of your contributions. See also WP:EVASION.
- **Contributing to the same page or discussion with multiple accounts**: Editors may not use more than one account to contribute to the same page or discussion in a way that suggests they are multiple people. Contributing to the same page with clearly linked, legitimate, alternative accounts (e.g. editing the same page with your main and public computer account or editing a page using your main account that your bot account edited) is not forbidden.
- **Avoiding scrutiny**: Using alternative accounts that are not fully and openly disclosed to split your editing history means that other editors may not be able to detect patterns in your contributions. While this is permitted in certain circumstances (see legitimate uses), it is a violation of this policy to create alternative accounts to confuse or deceive editors who may have a legitimate interest in reviewing your contributions.
- **"Good hand" and "bad hand" accounts**: Using one account for constructive contributions and the other one for disruptive editing or vandalism.
- **Editing while logged out in order to mislead**: Editing under multiple IP addresses may be treated as the same level of disruption as editing under multiple accounts when it is done deceptively or otherwise violates the principles of this policy. When editors log out by mistake, they may wish to contact an editor with oversight access to ensure there is no misunderstanding.
- **Misusing a clean start** by switching accounts or concealing a clean start in a way that avoids scrutiny is considered a breach of this policy; see Wikipedia:Clean start.
- **Role accounts**: Because an account represents your edits *as an individual*, "role accounts", or accounts shared by multiple people, are as a rule forbidden and blocked. Many first time editors may sign up an account with a username that implies it is a role account or is being shared. Such accounts are permitted only if the account information is forever limited to one individual; however, policy recommends that usernames avoid being misleading or disruptive. As such, if you edit for an organization, please refer to Wikipedia's username policy for guidance on choosing a name or a replacement name that can avoid these problems. Role account exceptions can be made for *non-editing* accounts approved to provide email access, accounts approved by the Wikimedia Foundation (list below), and approved bots with multiple managers. See Username policy – Sharing accounts.
- **Deceptively seeking positions of community trust**. You may not run for positions of trust without disclosing that you have previously edited under another account. Adminship reflects the community's trust in an individual, not an account, so when applying for adminship, it is expected that you will disclose past accounts openly, or email the arbitration committee if the accounts must be kept private. Administrators who fail to disclose past accounts risk being desysopped, particularly if knowledge of them would have influenced the outcome of the RfA.
- **Using more than one administrator account**: Editors may **not** have more than one account with administrator user rights, except for bots with administrator privileges. However, Foundation staff may operate more than one admin account, though they must make known who they are. If an administrator leaves the project, returns under a new username, and is nominated for adminship, he or she must resign or give up the administrator access of their old account.
- **Posing as a neutral or uninvolved commentator**: Using an alternative account to participate in a discussion about another account operated by the same person.

Legitimate uses

See also: the categories Wikipedians with alternative accounts and Wikipedia alternative accounts.

Alternative accounts have legitimate uses. For example, editors who contribute using their real name may wish to use a pseudonym for contributions with which they do not want their real name to be associated, or long-term users might create a new account to better understand the editing experience from a new user's perspective. These accounts are not considered sockpuppets. If you use a legitimate alternative account, it is your responsibility to ensure that you do not use it in an illegitimate manner according to this policy.

Valid reasons for an alternative account include:

- **Security**: You may register an alternative account for use when accessing Wikipedia through a public computer, connecting to an unsecured network, or other scenarios when there's a risk of your account being compromised. Such accounts should be publicly connected to the main account or use an easily identified name. For example, User:Mickey might use User:Mickey (alt) or User:Mouse, and redirect that account's user and talk pages to their main account.
- **Privacy**: A person editing an article which is highly controversial within his/her family, social or professional circle, and whose Wikipedia identity is known within that circle, or traceable to their real-world identity, may wish to use an alternative account to avoid real-world consequences from their editing or other Wikipedia actions in that area. Although a privacy-based alternative account is not publicly connected to your main account, it should not be used in ways outlined in the inappropriate uses section of this page, and if it is, the account may be publicly linked to your main account for sanctions. If you are considering using an alternative account under this provision, please read the notification section below.
- **Doppelgänger accounts**: A doppelgänger account is an account created with a username similar to your main account to prevent impersonation. Such accounts should not be used for editing. Doppelgänger accounts may be marked with the {{doppelganger}} or {{doppelganger-other}} tag, or can simply redirect to the main account's userpage.
- **Clean start under a new name**: A clean start is when a user stops using an old account in order to start afresh with a new account, usually due to past mistakes or to avoid harassment. A clean start is permitted only if there are no active bans, blocks, or sanctions in place against the old account. Do not use your new account to return to topic areas, disputes, editing patterns, or behaviors previously identified as problematic, and you should be careful not to do anything that looks like an attempt to evade scrutiny. A clean start requires that you no longer use your old account(s), which should note on their user pages that they are inactive—for example, with the {{retired}} tag—to prevent the switch being seen as an attempt to sock puppet.
- **Username violations**: If you are blocked for having an inappropriate username, and that is the sole reason for the block, you are permitted to create a new account with an appropriate username.
- **Compromised accounts**: If you are unable to access your account because you have lost the password or because someone has obtained or guessed your password, you may create a new account with a clean password. In such a case, you should post a note on the user page of each account indicating that they are alternative accounts for the same person. If necessary, you should also ask for an admin to block the compromised account. You may want to consider using a committed identity in advance to help deal with this rare situation should it arise later.
- **Humor accounts**: The community has accepted some obviously humorous alternate accounts, for example User:Bishzilla, User:Bishapod, User:Darwinbish, User:Darwinfish, User:Floquenstein's monster, and sometimes Lady Catherine Rollbacker-de Burgh (the Late).
- **Technical reasons**:
  - **Maintenance**: An editor might use an alternative account to carry out maintenance tasks, or to segregate functions so as to maintain a user talk page dedicated to the purpose. The second account should be clearly linked to the main account.
  - **Bots**: Bots are programs that edit automatically or semi-automatically. Editors who use bots are encouraged to create separate accounts, and ask that they be marked as bot accounts via

Wikipedia:Bots/Requests for approval, so that the automated edits can be filtered out of recent changes. Bots should be clearly linked to their owner's account. *See Wikipedia:Bot policy*.

- **Testing and training**: Users who use a lot of scripts and other tools may wish to keep a second, "vanilla" account, for testing how things appear to others; or for demonstrating Wikipedia's default appearance when training new users. The second account should be clearly linked to the main account, except where doing so would interfere with testing or training, e.g. creating an account named "user:example" to serve as an example account analogous to the website example.com.

- **Designated roles:** Editors with specific roles, such as Wikipedian in residence or Wikimedia Foundation employees, may have specific accounts for those roles. Note the account still belongs to an individual, not the role itself, and should be named as such. For example, *User:ExampleName (WIR for Foo Museum)* is an acceptable alternative account, but *User:Wikipedian-in-residence for Foo Museum* is not, because it is named after the role. It is not required that the names match, e.g. the main account *User:JohnDoe* could have the role account *User:ExampleName (WIR for Foo Museum)*, but the accounts should be clearly connected. If the editor leaves the role, their role account must no longer be used. If a new editor assumes the role, they must create a new account.
- **Teaching**: Teachers who incorporate Wikipedia into their classes may create an account for the purpose of supervising students. Use of the account should be limited to articles and other pages directly related to students and classwork.

Alternative accounts should always be identified as such on their user pages, except where doing so would defeat the point of the account. Templates such as {{User alternative account}} or one of a selection of user boxes may be used for this purpose.

Editing while logged out

See also: Help:Logging in § Editing while logged out

There is no policy against editing while logged out *per se*. This happens for many reasons, including not noticing that the login session had expired, changing computers, going to a Wikipedia page directly from a link, and forgetting passwords. Editors who are not logged in must not actively try to deceive other editors, such as by directly saying that they do not have an account or by using the session for the inappropriate uses of alternate accounts listed earlier in this policy. To protect their privacy, editors who have edited while logged out are never required to connect their usernames to their IP addresses on-wiki.

If you have concerns that an IP editor is actually a user with an account who is editing while logged out in a way that is inappropriate, you can give the IP editor notice of this policy (template for notification), and if the behavior continues, you should contact a CheckUser privately and present the evidence to them.

Alternative account notification

See also: Wikipedia:Userboxes/Wikipedia/Related accounts

Except when doing so would defeat the purpose of having a legitimate alternative account, editors using alternative accounts should provide links between the accounts. Links should ideally take the form of all three of the following:

1. Similarities in the username (for example, User:Example might have User:Example public or User:Example bot).[3]
2. Links on both the main and alternative account user pages, either informally or using the userbox templates made for the purpose. To link an alternative account to a main account, use the **main** account to tag any secondary accounts with {{User alternate acct | *main account*}} (using the main account shows

it's genuine) or {{Public user}} if the account is being used to maintain security on public computers. The main account may be marked with {{User alternative account name|*OtherName*|...|*OtherName[n]*}} or {{User Alt Acct Master}}.

3. Links in the alternative account signature: if not linking to both the alternative and main account, link to the alternative account, and if necessary provide a note there requesting contact be made via the main account, or simply redirect the user talk page.

Editors who have multiple accounts for privacy reasons should *consider* notifying a checkuser or members of the arbitration committee if they believe editing will attract scrutiny. Editors who heavily edit controversial material, those who maintain single purpose accounts, as well as editors considering becoming an administrator are among the groups of editors who attract scrutiny even if their editing behavior itself is not problematic or only marginally so. Concerned editors may wish to email the arbitration committee or any individual with checkuser rights (https://en.wikipedia.org/w/index.php?title=Special%3AListUsers&group=checkuser). Editors who have abandoned an account and are editing under a new identity are required to comply with the clean start policy.

Meatpuppetry

See also: Wikipedia:Canvassing



This section in a nutshell: Do not recruit your friends, family members, or communities of people who agree with you for the purpose of coming to Wikipedia and supporting your side of a debate. If you feel that a debate is ignoring your voice, remain civil, and seek comments from other Wikipedians or pursue dispute resolution. These are well-tested processes, designed to avoid the problem of exchanging bias in one direction for bias in another.

High-profile disputes on Wikipedia often bring new editors to the site. Some individuals may promote their causes by bringing like-minded editors into the dispute. These editors are sometimes referred to as *meatpuppets*, following a common Internet usage. While Wikipedia assumes good faith, especially for new users, recruiting new editors to influence decisions on Wikipedia is prohibited. A new user who engages in the same behavior as another user in the same context, and who appears to be editing Wikipedia solely for that purpose, may be subject to the remedies applied to the user whose behavior they are joining. Sanctions have been applied to editors of longer standing who have not, in the opinion of Wikipedia's administrative bodies, consistently exercised independent judgment.

Wikipedia has processes in place to mitigate the disruption caused by an influx of single-purpose editors:

- Consensus in many debates and discussions should ideally **not** be based upon number of votes, but upon policy-related points made by editors.
- In votes or vote-like discussions, new users may be disregarded or given significantly less weight, especially if there are many of them expressing the same opinion. Their comments may be tagged with a note pointing out that they have made few or no other edits outside of the discussion.
- A 2005 Arbitration Committee decision established that "for the purpose of dispute resolution when there is uncertainty whether a party is one user with sockpuppets or several users with similar editing habits they may be treated as one user with sockpuppets."[4]

The term *meatpuppet* may be seen by some as derogatory and should be used with care, in keeping with Wikipedia's civility policy. Because of the processes above, it may be counterproductive to directly accuse someone of being a "meatpuppet", and doing so will often only inflame the dispute.

Sharing an IP address

"WP:SHARE" redirects here. For the policy prohibiting the sharing of accounts, see Wikipedia:Username policy § Sharing accounts. For the sharebox script, see User:TheDJ/Sharebox.

If two or more registered editors use the same computer or network connection, their accounts may be linked by a CheckUser. Editors in this position are advised to declare such connections on their user pages to avoid accusations of sockpuppetry. There are userboxes available for this; see {{User shared IP address}}.

Closely connected users may be considered a single user for Wikipedia's purposes if they edit with the same objectives. When editing the same articles, participating in the same community discussion, or supporting each other in any sort of dispute, closely related accounts should disclose the connection and observe relevant policies such as edit warring as if they were a single account. If they do not wish to disclose the connection, they should avoid editing in the same areas, particularly on controversial topics.

Handling suspected sock puppets

Sockpuppet investigations

Wikipedia:Signs of sock puppetry lists some of the signs that an account may be a sock puppet. If you believe someone is using sock puppets or meat puppets, you should create a report at Wikipedia:Sockpuppet investigations. In reporting suspected sock puppetry, you must obey the rules of WP:OUTING with regard to disclosure of personal or identifying information. Only blocked accounts should be tagged as Category:Suspected Wikipedia sockpuppets and only upon sufficient evidence that would stand up to scrutiny.

CheckUser

Further information: Wikipedia:CheckUser

Editors with access to the CheckUser tool may consult the server log to see which IP addresses are linked to which accounts. CheckUser cannot confirm with certainty that two accounts are not connected; it

Sockpuppet investigations

Current cases

Sock puppetry policy

Information pages

Guide to filing cases

Administrator instructions

Signs of sock puppetry

SPI clerk pages

List of clerks

Noticeboard (archive 1, archive 2, archive 3)

Procedures

Training

SPI archives

Archived cases (historical)

Malformed Cases (whitelist)

Search all archives Go

can only show whether there is a technical link at the time of the check. In accordance with the Wikimedia Foundation's Privacy and Checkuser policies, checks are only conducted with good cause, and (subject to the exceptions in those policies) results are reported in such a way as to avoid or minimize disclosure of personal identifying information. Particularly, "fishing"—the use of CheckUser without good cause specific to a given user account—is prohibited.

Blocking

Further information: Wikipedia:Blocking policy

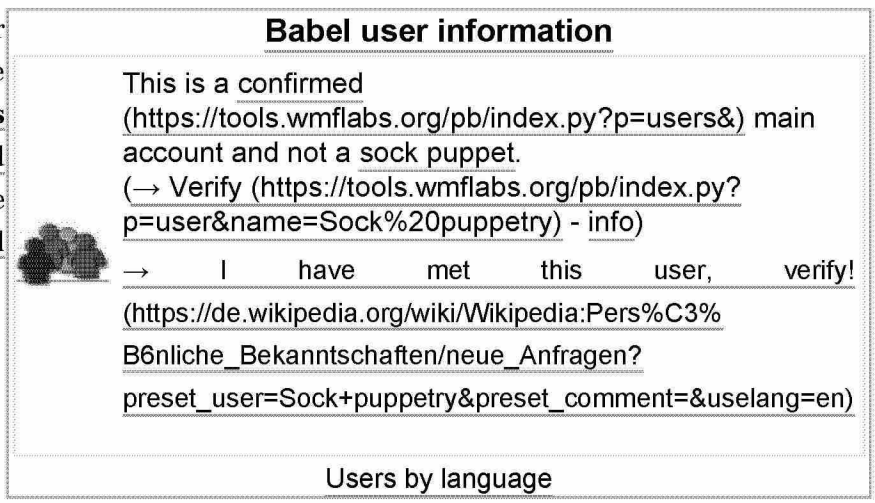
If a person is found to be using a sock puppet, the sock puppet account(s) should be blocked indefinitely. The main account may be blocked at the discretion of any uninvolved administrator. IP addresses used for sock puppetry may be blocked, but are subject to certain restrictions for indefinite blocks.

Tagging

Further information: Wikipedia:Sockpuppet investigations/SPI/Administrators instructions § Blocking and tagging

Proving you are not a sock

One possibility to prove that your account is not a sock puppet is the **Personal acquaintances** WikiProject. This project was started in 2008 in the German language Wikipedia and uses a WMF labs tool



(https://tools.wmflabs.org/pb/beta/) where users can confirm that they have met a real person operating one specific Wikipedia or Wikimedia account at a meetup in real life. The project and its tool meanwhile have been translated to several other languages and can be accessed with any account using the global single user login. Once you have registered as a participant (https://de.wikipedia.org/wiki/Wikipedia:Persönliche_Bekanntschaften/neue_Anfragen?uselang=en) of *Personal acquaintances*, you need to be confirmed by three other participants in good standing before you can start confirming other real life persons yourself. For further information go to the project page linked above. You can show other Wikipedians that you are a real person by displaying the userbox {{Template:User Personal acquaintances}} on your userpage or the link to your list of confirmations via the url "https://tools.wmflabs.org/pb/beta/user/name/*your username*/".

List of role accounts

- *Non-editing accounts that provide an easy way to contact internal email lists:*
  - User:Arbitration Committee
  - User:Ban Appeals Subcommittee
  - User:Bureaucrats
  - User:Emergency
  - User:Mediation Committee[5]
  - User:Oversight
  - User:Wikipedia Information Team
  - User:Accounts-enwiki-l
- *Accounts approved by the Foundation:*

Category:Wikipedia contact role accounts

See also

- smurf account
- Sockpuppet (Internet)
- Wikipedia:Sleeper accounts
- Wikipedia:Sockpuppet investigations

Guidelines

- Wikipedia:Canvassing

Essays

- Wikipedia:Anything to declare?
- Wikipedia:Cabals
- Wikipedia:Consequences of sock puppetry
- Wikipedia:Don't be quick to assume that someone is a sockpuppet
- Wikipedia:Griefing
- Wikipedia:Lurkers
- Wikipedia:On privacy, confidentiality and discretion
- Wikipedia:Signs of sock puppetry
- Wikipedia:Single-purpose account
- Wikipedia:Tag team
- Wikipedia:The duck test

References

1. Wikimedia Foundation privacy policy:

> "We hope that this never comes up, but we may disclose your personal information if we believe that it's reasonably necessary [...] to protect our organization, employees, contractors, users, or the public. We may also disclose your personal information if we reasonably believe it necessary to detect, prevent, or otherwise assess and address potential spam, malware, fraud, abuse, unlawful activity, and security or technical concerns."

Information under this policy is not gratuitously released, but may be made public at times in the context of detecting, confirming, preventing, and resolving issues related to actual or possible abuse.

2. See Wikipedia:Requests for arbitration/Privatemusings#Sockpuppetry.
3. Dissimilar names may cause confusion and create an impression of avoiding transparency; remember that the username appears in page histories even if you change the signature.
4. Wikipedia:Requests for arbitration/Regarding Ted Kennedy#Sockpuppets
5. Ownership of this account is passed between outgoing and newly-appointed Chairpersons, and the password is changed upon the transferral of ownership, so this is not a "role account".

External links

- MeatBall:SockPuppet

Wikipedia key policies and guidelines

Five pillars (What Wikipedia is not · Ignore all rules)

Content	✓	Verifiability · No original research · Neutral point of view · What Wikipedia is not · Biographies of living persons · Image use · Wikipedia is not a dictionary · Article titles
	✓	Notability · Autobiography · Citing sources · Identifying reliable sources (medicine) · Do not include copies of primary sources · Plagiarism · Don't create hoaxes · Fringe theories · Patent nonsense · External links
Conduct	✓	Civility · Consensus · Editing policy · Harassment · Vandalism · Ignore all rules · No personal attacks · Ownership of content · Edit warring · Dispute resolution · Sock puppetry · No legal threats · Child protection · Paid-contribution disclosure
	✓	Assume good faith · Conflict of interest · Disruptive editing · Do not disrupt Wikipedia to illustrate a point · Etiquette · Gaming the system · Please do not bite the newcomers · Courtesy vanishing
Deletion	✓	Deletion policy · Proposed deletion · Criteria for speedy deletion · Attack page · Oversight · Proposed deletion of BLP · Proposed deletion (books) · Revision deletion
Enforcement	✓	Administrators · Banning · Blocking · Page protection
Editing	✓	

		Article size · Be bold · Disambiguation · Hatnotes · Set index articles · Subpages · User pages · Talk page guidelines (Signatures) · Broad-concept article · Project namespace (WikiProjects)
	Style	Manual of Style (Contents) · Accessibility (Understandability) · Dates and numbers · Images · Layout · Lead section · Linking · Lists
	Classification	Categories, lists, and navigation templates · Categorization · Template namespace
WMF	✓	List of policies · Friendly space policy · Licensing and copyright · Privacy policy · Values · FAQ

List of all policies and guidelines (✓ List of policies · ✓ List of guidelines) · Lists of attempts in creating fundamental principles

Sock puppetry

Guidance	Legitimate uses · Inappropriate uses · Meat puppetry · Canvassing · Username policy · Clean start · Single-purpose account · Sleeper accounts · Outing
Signs	Motivations · List of signs · Duck test · An obvious sock is obvious · Don't be quick to assume that someone is a sockpuppet · Lurkers
Investigations	Triggers · Administrators instructions · Requests for checkuser · CheckUser criteria
Consequences	Block · Ban

Wikipedia accounts and governance

Unregistered (IP) users	Why create an account? · Create an account · Request an account · IPs are human too · IP addresses are not people · IP hopper
Registered users	New account · Logging in (Reset passwords) · Username policy (Changing username · Usernames for administrator attention) · Unified login or SUL · Alternate account
Account security	Password strength requirements · User account security · Personal security practices · Two-factor authentication (Simple 2FA · 2FA for AWB) · Committed identity · On privacy, confidentiality and discretion · Compromised accounts
Blocks, global locks, bans, sanctions	Blocking policy (FAQ · Admins guide · Tools · Autoblock) · Appealing a block (Guide to appealing blocks · UTRS Unblock Ticket Request System) · Blocking IP addresses (Range blocks · IPv6 · Open proxies) · Global locks · Banning policy (ArbCom appeals) · Sanctions (Personal sanctions · General sanctions · Discretionary sanctions and Log · Essay) · Long-term abuse · Standard offer

Related to accounts	Sock puppetry · Single-purpose account · Sleeper account · Vandalism-only account · Wikibreak (Enforcer) · Retiring (Courtesy vanishing) · Clean start (Quiet return)
User groups and global user groups	Requests for permissions (Admin instructions · Admin guide) · Account creator (PERM) · Autopatrolled (PERM) · AutoWikiBrowser (PERM) · Confirmed (PERM) · Extended confirmed (PERM) · Edit filter helper · File mover (PERM) · Mass message sender (PERM) · New page reviewer (PERM) · Page mover (PERM) · Pending changes reviewer (PERM) · Rollback (PERM) · Template editor (PERM) · IP-block-exempt (Requests) · Courses access (Requests) · Bot accounts (Requests) · Global rights policy (OTRS Volunteer Response Team)
Advanced user groups	Administrators (RfA) · Bureaucrats (RfB) · Edit filter manager (Requests) · CheckUser and Oversight (Requests) · Founder
Committees and related	Arbitration Committee · Mediation Committee · Bot approvals group · Functionaries · Clerks
Governance	Administration (FAQ) · Formal organization · Editorial oversight and control · Quality control · Wikimedia Foundation (Board · Founder's seat · Meta-Wiki) · Leadership opportunities · WikiProjects · Elections · Policies and guidelines · Unbundling administrators' powers · Petitions · Noticeboards · Consensus · Dispute resolution · Reforms

Retrieved from "https://en.wikipedia.org/w/index.php?title=Wikipedia:Sock_puppetry&oldid=829183984"

This page was last edited on 7 March 2018, at 03:47.

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

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

Plaintiff's Exhibit 35

Privacy policy

العربية | azərbaycanca | تورکجه | български | روچ کپتین بلوچی | বাংলা | bosanski | català | нохчийн | کوردی | čeština | català | Cymraeg | Deutsch | Deutsch (Sie-Form) | Zazaki | Ελληνικά | emiliàn e rumagnòl | English | Canadian English | British English | Esperanto | español | euskara | فارسی | suomi | français | Nordfriisk | Frysk | galego | Avañe'ẽ | עברית | हिन्दी | hrvatski | magyar | Bahasa Indonesia | italiano | 日本語 | ქართული | ភាសាខ្មែរ | 한국어 | Ripoarisch | Кыргызча | Lëtzebuergesch | Ligure | lietuvių | Basa Banyumasan | македонски | മലയാളം | Bahasa Melayu | မြန်မာဘာသာ | مازرونی | Napulitano | norsk bokmål | नेपाली | Nederlands | nl-formal | Diné bizaad | occitan | ਪੰਜਾਬੀ | Plautdietsch | polski | پښتو | português | português do Brasil | română | русский | Scots | سنڌي | ဘာသာမန် | සිංහල | Soomaaliga | shqip | српски / srpski | svenska | Kiswahili | தமிழ் | తెలుగు | тоҷикӣ | ไทย | Türkçe | удмурт | українська | اردو | Tiếng Việt | მარგალური | ייִדיש | Yorùbá | 粵語 | 中文 | 中文（简体） | 中文（繁體）

This policy is approved by the Wikimedia Foundation Board of Trustees to apply to all Wikimedia projects. It may not be circumvented, eroded, or ignored by local policies.

Want to help translate? Translate the missing messages.

This is a summary of the Privacy Policy. To read the full terms, click here.

Disclaimer: This summary is not a part of the Privacy Policy and is not a legal document. It is simply a handy reference for understanding the full Privacy Policy. Think of it as the user-friendly interface to our Privacy Policy.

Because we believe that you shouldn't have to provide personal information to participate in the free knowledge movement, you may:

- Read, edit, or use any Wikimedia Site without registering an account.
- Register for an account without providing an email address or real name.

Because we want to understand how Wikimedia Sites are used so we can make them better for you, we collect some information when you:

- Make public contributions.
- Register an account or update your user page.
- Use the Wikimedia Sites.
- Send us emails or participate in a survey or give feedback.

We are committed to:

- Describing how your information may be used or shared in this Privacy Policy.
- Using reasonable measures to keep your information secure.
- Never selling your information or sharing it with third parties for marketing purposes.
- Only sharing your information in limited circumstances, such as to improve the Wikimedia Sites, to comply with the law, or to protect you and others.

- Retaining your data for the shortest possible time that is consistent with maintaining, understanding, and improving the Wikimedia Sites, and our obligations under law.

Be aware:

- Any content you add or any change that you make to a Wikimedia Site will be publicly and permanently available.
- If you add content or make a change to a Wikimedia Site without logging in, that content or change will be publicly and permanently attributed to the IP address used at the time rather than a username.
- Our community of volunteer editors and contributors is a self-policing body. Certain administrators of the Wikimedia Sites, who are chosen by the community, use tools that grant them limited access to nonpublic information about recent contributions so they may protect the Wikimedia Sites and enforce policies.
- This Privacy Policy does not apply to all sites and services run by the Wikimedia Foundation, such as sites or services that have their own privacy policy (like the Wikimedia Shop (https://shop.wikimedia.org)) or sites or services run by third parties (like third-party developer projects on Wikimedia Cloud Services).
- As part of our commitment to education and research around the world, we occasionally release public information and aggregated or non-personal information to the general public through data dumps and data sets.
- For the protection of the Wikimedia Foundation and other users, if you do not agree with this Privacy Policy, you may not use the Wikimedia Sites.

Introduction Use of info Sharing Protection Important info

Contents [show]

Introduction

Welcome!

The Wikimedia Foundation is the nonprofit organization that operates collaborative, free knowledge websites, like

Wikipedia, Wikimedia Commons, and Wiktionary.

This Policy explains how we collect, use, and share your personal information.

- We collect very little personal information about you.
- We do not rent or sell your information to third parties.

By using Wikimedia Sites, you consent to this Policy.

The Wikimedia movement is founded on a simple, but powerful principle: we can do more together than any of us can do alone. We cannot work collectively without gathering, sharing, and analyzing information about our users as we seek new ways to make the Wikimedia Sites more useable, safer, and more beneficial.

We believe that information-gathering and use should go hand-in-hand with transparency. This Privacy Policy explains how the Wikimedia Foundation, the non-profit organization that hosts the Wikimedia Sites, like Wikipedia, collects, uses, and shares information we receive from you through your use of the Wikimedia Sites. It is essential to understand that, by using any of the Wikimedia Sites, you consent to the collection, transfer, processing, storage, disclosure, and use of your information as described in this Privacy Policy. That means that reading this Policy carefully is important.

We believe that you shouldn't have to provide personal information to participate in the free knowledge movement. You do not have to provide things like your real name, address, or date of birth to sign up for a standard account or contribute content to the Wikimedia Sites.

We do not sell or rent your nonpublic information, nor do we give it to others to sell you anything. We use it to figure out how to make the Wikimedia Sites more engaging and accessible, to see which ideas work, and to make learning and contributing more fun. Put simply: we use this information to make the Wikimedia Sites better for you.

After all, it's people like you, the champions of free knowledge, who make it

possible for the Wikimedia Sites to not only exist, but also grow and thrive.

Definitions

Because everyone (not just lawyers) should be able to easily understand how and why their information is collected and used, we use common language instead of more formal terms throughout this Policy. To help ensure your understanding of some particular key terms, here is a table of translations:

When we say...	... we mean:
"the Wikimedia Foundation" / "the Foundation" / "we" / "us" / "our"	The Wikimedia Foundation, Inc., the non-profit organization that operates the Wikimedia Sites.
"Wikimedia Sites" / "our services"	Wikimedia websites and services (regardless of language), including our main projects, such as Wikipedia and Wikimedia Commons, as well as mobile applications, APIs, emails, and notifications; excluding, however, sites and services listed in the "What This Privacy Policy Doesn't Cover" section below.
"you" / "your" / "me"	You, regardless of whether you are an individual, group, or organization, and regardless of whether you are using the Wikimedia Sites or our services on behalf of yourself or someone else.
"this Policy" / "this Privacy Policy"	This document, entitled the "Wikimedia Foundation Privacy Policy".
"contributions"	Content you add or changes you make to any Wikimedia Sites.
"personal information"	Information you provide us or information we collect from you that could be used to personally identify you. To be clear, while we do not necessarily collect all of the following types of information, we consider at least the following to be “personal information” if it is otherwise nonpublic and can be used to identify you: (a) your real name, address, phone number, email address, password, identification number on government-issued ID, IP address, user-agent information, credit card number; (b) when associated with one of the items in subsection (a), any sensitive data such as date of birth, gender, sexual orientation, racial or ethnic origins, marital or familial status, medical conditions or disabilities, political affiliation, and religion; and (c) any of the items in subsections (a) or (b) when associated with your user account.
"third party" / "third parties"	Individuals, entities, websites, services, products, and applications that are not controlled, managed, or operated by the Wikimedia Foundation. This includes other Wikimedia users and independent organizations or groups who help promote the Wikimedia movement such as Wikimedia chapters, thematic organizations, and user groups as well as volunteers, employees, directors, officers, grant recipients, and contractors of those organizations or groups.

We recognize that only a minority of you are familiar with technical terms like "tracking pixels" and "cookies" used in the Privacy Policy. Whether you are brand new to privacy terminology or you are an expert who just wants a refresher, you might find our Glossary of Key Terms helpful.

What This Privacy Policy Does & Doesn't Cover

Except as explained below, this Privacy Policy applies to our collection and handling of information about you that we receive as a result of your use of any of the Wikimedia Sites. This Policy also applies to information that we receive from our partners or other third parties. To understand more about what this Privacy Policy covers, please see below.

Examples of What This Privacy Policy Covers [Expand]

This Privacy Policy, however, does not cover some situations where we may gather or process information. For example, some uses may be covered by separate privacy policies (like those of the Wikimedia Shop (https://store.wikimedia.org)) or sites or services run by third parties (such as third-party developer projects on Wikimedia Cloud Services). To understand more about what this Privacy Policy does not cover, please see below.

More on what this Privacy Policy doesn't cover [Expand]

Where community policies govern information, such as the CheckUser policy, the relevant community may add to the rules and obligations set out in this Policy. However, they are not permitted to create new exceptions or otherwise reduce the protections offered by this Policy.

Back to top

Use of info

Types of Information We Receive From You, How We Get It, & How We Use It

Your Public Contributions

Whatever you post on Wikimedia Sites can be seen and used by everyone.

The Wikimedia Sites were primarily created to help you share your knowledge with the world, and we share your contributions because you have asked us to do so.

When you make a contribution to any Wikimedia Site, including on user or discussion pages, you are creating a permanent, public record of every piece of content added, removed, or altered by you. The page history will show when your contribution or deletion was made, as well as your username (if you are signed in) or your IP address (if you are not signed in). We may use your public contributions, either aggregated with the public contributions of others or individually, to create new features or data-related products for you or to learn more about how the Wikimedia Sites are used.

Unless this Policy says otherwise, you should assume that information that you actively contribute to the Wikimedia Sites, including personal information, is publicly visible and can be found by search engines. Like most things on the Internet, anything you share may be copied and redistributed throughout the Internet by other people. Please do not contribute any information that you are uncomfortable making permanently public, like revealing your real name or location in your contributions.

You should be aware that specific data made public by you or aggregated data that is made public by us can be used by anyone for analysis and to infer information about users, such as which country a user is from, political affiliation, and gender.

Back to top

Account Information & Registration

You do not need to create an account to use any Wikimedia Site.

If you do create an account, you do not need to give us your name or email address.

If you do not create an account, your contributions will be publicly attributed to your IP address.

Want to create an account? Great! Don't want to create an account? No problem!

You are not required to create an account to read or contribute to a Wikimedia Site, except under rare circumstances. However, if you contribute without signing in, your contribution will be publicly attributed to the IP address associated with your device.

If you want to create a standard account, in most cases we require only a username and a password. Your username will be publicly visible, so please be careful about using your real name as your username. Your password is only used to verify that the account is yours. Your IP address is also automatically submitted to us, and we record it temporarily to help prevent abuse. No other personal information is required: no name, no email address, no date of birth, no credit card information.

Once created, user accounts cannot be removed entirely (although you can usually hide the information on your user page if you choose to). This is because your public contributions must be associated with their author (you!). So make sure you pick a name that you will be comfortable with for years to come.

To gain a better understanding of the demographics of our users, to localize our services, and to learn how we can improve our services, we may ask you for more demographic information, such as gender or age, about yourself. We will tell you if such information is intended to be public or private, so that you can make an informed decision about whether you want to provide us with that information. Providing such information is always completely optional. If you don't want to, you don't have to—it's as simple as that.

Back to top

Information Related to Your Use of the Wikimedia Sites

We may use common technologies to collect information about how you use Wikimedia Sites.

We use this information to enhance your user experience and to develop new features.

We want to make the Wikimedia Sites better for you by learning more about how you use them. Examples of this might include how often you visit the Wikimedia Sites, what you like, what you find helpful, how you get to the Wikimedia Sites, and whether you would use a helpful feature more if we explained it differently. We also want this Policy and our practices to reflect our community's values. For this reason, we keep information related to your use of the Wikimedia Sites confidential, except as provided in this Policy.

Back to top

Information We Receive Automatically

Like other websites, we receive some information about you automatically when you visit the Wikimedia Sites. This information helps us administer the Wikimedia Sites and enhance your user experience.

Because of how browsers work and similar to other major websites, we receive some information automatically when you visit the Wikimedia Sites. This information includes the type of device you are using (possibly including unique device identification numbers, for some beta versions of our mobile applications), the type and version of your browser, your browser's language preference, the type and version of your device's operating system, in some cases the name of your internet service provider or mobile carrier, the website that referred you to the Wikimedia Sites, which pages you request and visit, and the date and time of each request you make to the Wikimedia Sites.

Put simply, we use this information to enhance your experience with Wikimedia Sites. For example, we use this information to administer the sites, provide greater security, and fight vandalism; optimize mobile applications, customize content and set language preferences, test features to see what works, and improve performance; understand how users interact

with the Wikimedia Sites, track and study use of various features, gain understanding about the demographics of the different Wikimedia Sites, and analyze trends.

Back to top

Information We Collect

We use a variety of commonly-used technologies, like cookies, to understand how you use the Wikimedia Sites, make our services safer and easier to use, and to help create a better and more personalized experience for you.

We actively collect some types of information with a variety of commonly-used technologies. These generally include tracking pixels, JavaScript, and a variety of "locally stored data" technologies, such as cookies and local storage. We realize that some of these technologies do not have the best reputation in town and can be used for less-than-noble purposes. So we want to be as clear as we can about why we use these methods and the type of information we collect with them.

Depending on which technology we use, locally stored data can be anything from text, pictures, and whole articles (as we explain further below) to personal information (like your IP address) and information about your use of the Wikimedia Sites (like your username or the time of your visit).

We use this information to make your experience with the Wikimedia Sites safer and better, to gain a greater understanding of user preferences and their interaction with the Wikimedia Sites, and to generally improve our services. We will never use third-party cookies, unless we get your permission to do so. If you ever come across a third-party data collection tool that has not been authorized by you (such as one that may have been mistakenly placed by another user or administrator), please report it to us at privacy@wikimedia.org (mailto:privacy@wikimedia.org).

Locally stored data, JavaScript, and tracking pixels help us do things like:

- Provide you with a personalized experience, such as using cookies to know your language preference, to remember the user preferences you

set so we can provide you with the customized look and feel that you want, and to tell you about interesting Wikimedia issues and events in your area.

- Deliver more relevant content to you faster. For example, we may use local storage to store your most recently read articles directly on your device, so they can be retrieved quickly. Also, we may use cookies to learn about the topics searched so that we can optimize the search results we deliver to you.
- Understand how you use the Wikimedia Sites, so that we know what works and what is useful. For example, we might use cookies to learn about the list of articles you are following on your watchlist so that we can recommend similar articles that you may be interested in.
- Understand how you use the Wikimedia Sites across different devices, so that we can make our varied Wikimedia Sites more efficient and effective for you.
- Make the Wikimedia Sites more convenient to use, such as by using cookies to maintain your session when you log in or to remember your username in the login field.

Want to know even more? You can read more about some of the specific cookies we use, when they expire, and what we use them for in our FAQ.

We believe this data collection helps improve your user experience, but you may remove or disable some or all locally stored data through your browser settings, depending on your browser. You can learn more about some options you have in our FAQ. While locally stored data may not be necessary to use our sites, some features may not function properly if you disable locally stored data.

While the examples above concerning information about you collected through the use of data collection tools are kept confidential in accordance with this Policy, please note that some information about the actions taken by your username is made publicly available through public logs alongside actions taken by other users. For example, a public log may include the date your account was created on a Wikimedia Site along with the dates that other accounts were created on a Wikimedia Site. Information available through public logs will not include personal information about you.

Back to top

Emails

If you choose to provide your email address, we will keep it confidential, except as provided in this Policy.

We may occasionally send you emails about important information.

You may choose to opt out of certain kinds of notifications.

You have the option of providing an email address at the time of registration or in later interactions with the Wikimedia Sites. If you do so, your email address is kept confidential, except as provided in this Policy. We do not sell, rent, or use your email address to advertise third-party products or services to you.

We use your email address to let you know about things that are happening with the Foundation, the Wikimedia Sites, or the Wikimedia movement, such as telling you important information about your account, letting you know if something is changing about the Wikimedia Sites or policies, and alerting you when there has been a change to an article that you have decided to follow. Please note that if you email us, we may keep your message, email address, and any other information you provide us, so that we can process and respond to your request.

You can choose to limit some of these kinds of notifications, like those alerting you if an article changes. Others, such as those containing critical information that all users need to know to participate successfully in the Wikimedia Sites, you may not be able to opt out of. You can manage what kinds of notifications you receive and how often you receive them by going to your Notifications Preferences. You can learn more about email and notifications and how to change your preferences in our FAQ.

We will never ask for your password by email (but may send you a temporary password via email if you have requested a password reset). If you ever receive such an email, please let us know by sending it to privacy@wikimedia.org (mailto:privacy@wikimedia.org), so we can investigate the source of the email.

Direct communications between users (such as messages sent through the "Email this user" feature), to the extent such communications are nonpublic and stored in or in transit through Wikimedia Foundation systems, are kept confidential by us, except as provided in this Policy.

Back to top

Surveys & Feedback

We may ask you to provide us with information through a survey or provide feedback, but you will never be obligated to participate.

Participating in optional surveys or providing feedback helps us make the Wikimedia Sites better. Because every survey and request for feedback may be used for various purposes, we will tell you, at the time we give you the survey or request for feedback, how we plan on using your answers and any personal information you provide. If you don't feel comfortable with how we plan on using the survey or feedback results, you are not obligated to take the survey or give feedback.

Back to top

Location Information

GPS & Other Location Technologies

If you consent, we can use commonly-used location technologies to show you more relevant content.

Some features we offer work better if we know what area you are in. But it's completely up to you whether or not you want us to use geolocation tools to make some features available to you. If you consent, we can use GPS (and other technologies commonly used to determine location) to show you more relevant content. We keep information obtained by these technologies confidential, except as provided in this Policy. You can learn more by checking out the list of examples of how we use these technologies in our FAQ.

Back to top

Metadata

We may automatically receive location data from your device. For example, if you upload a photo using the Wikimedia Commons mobile app, please be aware that the default setting on your mobile device typically results in the metadata associated with your photo being included in the upload.

Sometimes, we may automatically receive location data from your device. For example, if you want to upload a photo on the Wikimedia Commons mobile app, we may receive metadata, such as the place and time you took the photo, automatically from your device. Please be aware that, unlike location information collected using GPS signals described above, the default setting on your mobile device typically includes the metadata in your photo or video upload to the Wikimedia Sites. If you do not want metadata sent to us and made public at the time of your upload, please change your settings on your device.

Back to top

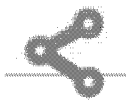
IP Addresses

When you visit any Wikimedia Site, we automatically receive the IP address of the device you are using to access the Internet, which can be used to infer your geographical location.

Finally, when you visit any Wikimedia Site, we automatically receive the IP address of the device (or your proxy server) you are using to access the Internet, which could be used to infer your geographical location. We keep IP addresses confidential, except as provided in this Policy. For example, if you make a contribution without signing into your account, your IP address used at the time will be publicly and permanently recorded. If you are visiting

Wikimedia Sites with your mobile device, we may use your IP address to provide anonymized or aggregated information to service providers regarding the volume of usage in certain areas. We use IP addresses for research and analytics; to better personalize content, notices, and settings for you; to fight spam, identity theft, malware, and other kinds of abuse; and to provide better mobile and other applications.

Back to top



Sharing

When May We Share Your Information?

We may share your information when you give us specific permission to do so.

With Your Permission

We may share your information for a particular purpose, if you agree. You can find more information in the list of examples in our FAQ.

Back to top

For Legal Reasons

We will disclose your information in response to an official legal process only if we believe it to be legally valid. We will notify you of such requests when possible.

We may access, preserve, or disclose your personal information if we reasonably believe it necessary to satisfy a valid and legally enforceable warrant, subpoena, court order, law or regulation, or other judicial or administrative order. However, if we believe that a particular request for disclosure of a user's information is legally invalid or an abuse of the legal

system and the affected user does not intend to oppose the disclosure themselves, we will try our best to fight it. We are committed to notifying you via email at least ten (10) calendar days, when possible, before we disclose your personal information in response to a legal demand. However, we may only provide notice if we are not legally restrained from contacting you, there is no credible threat to life or limb that is created or increased by disclosing the request, and you have provided us with an email address.

Nothing in this Privacy Policy is intended to limit any legal objections or defenses you may have to a third party's request (whether it be civil, criminal, or governmental) to disclose your information. We recommend seeking the advice of legal counsel immediately if such a request is made involving you.

For more information, see our Subpoena FAQ.

Back to top

If the Organization is Transferred (Really Unlikely!)

In the unlikely event that the ownership of the Foundation changes, we will provide you 30 days notice before any personal information is transferred to the new owners or becomes subject to a different privacy policy.

In the extremely unlikely event that ownership of all or substantially all of the Foundation changes, or we go through a reorganization (such as a merger, consolidation, or acquisition), we will continue to keep your personal information confidential, except as provided in this Policy, and provide notice to you via the Wikimedia Sites and a notification on WikimediaAnnounce-L or similar mailing list at least thirty (30) calendar days before any personal information is transferred or becomes subject to a different privacy policy.

Back to top

To Protect You, Ourselves & Others

We, or users with certain administrative rights, may disclose information that is reasonably necessary to:

- enforce or investigate potential violations of Foundation or community-based policies;
- protect our organization, infrastructure, employees, contractors, or the public; or
- prevent imminent or serious bodily harm or death to a person.

We, or particular users with certain administrative rights as described below, may need to share your personal information if it is reasonably believed to be necessary to enforce or investigate potential violations of our Terms of Use, this Privacy Policy, or any Foundation or user community-based policies. We may also need to access and share information to investigate and defend ourselves against legal threats or actions.

Wikimedia Sites are collaborative, with users writing most of the policies and selecting from amongst themselves people to hold certain administrative rights. These rights may include access to limited amounts of otherwise nonpublic information about recent contributions and activity by other users. They use this access to help protect against vandalism and abuse, fight harassment of other users, and generally try to minimize disruptive behavior on the Wikimedia Sites. These various user-selected administrative groups have their own privacy and confidentiality guidelines, but all such groups are supposed to agree to follow our Access to Nonpublic Information Policy. These user-selected administrative groups are accountable to other users through checks and balances: users are selected through a community-driven process and overseen by their peers through a logged history of their actions. However, the legal names of these users are not known to the Wikimedia Foundation.

We hope that this never comes up, but we may disclose your personal information if we believe that it's reasonably necessary to prevent imminent and serious bodily harm or death to a person, or to protect our organization, employees, contractors, users, or the public. We may also disclose your personal information if we reasonably believe it necessary to detect, prevent,

or otherwise assess and address potential spam, malware, fraud, abuse, unlawful activity, and security or technical concerns. (Check out the list of examples in our FAQ for more information.)

Back to top

To Our Service Providers

We may disclose personal information to our third-party service providers or contractors to help run or improve the Wikimedia Sites and provide services in support of our mission.

As hard as we may try, we can't do it all. So sometimes we use third-party service providers or contractors who help run or improve the Wikimedia Sites for you and other users. We may give access to your personal information to these providers or contractors as needed to perform their services for us or to use their tools and services. We put requirements, such as confidentiality agreements, in place to help ensure that these service providers treat your information consistently with, and no less protective of your privacy than, the principles of this Policy. (Check out the list of examples in our FAQ.)

Back to top

To Understand & Experiment

We may give volunteer developers and researchers access to systems that contain your information to allow them to protect, develop, and contribute to the Wikimedia Sites.

We may also share non-personal or aggregated information with third

parties interested in studying the Wikimedia Sites.

When we share information with third parties for these purposes, we put reasonable technical and contractual protections in place to protect your information consistent with this Policy.

The open-source software that powers the Wikimedia Sites depends on the contributions of volunteer software developers, who spend time writing and testing code to help it improve and evolve with our users' needs. To facilitate their work, we may give some developers limited access to systems that contain your personal information, but only as reasonably necessary for them to develop and contribute to the Wikimedia Sites.

Similarly, we may share non-personal or aggregated information with researchers, scholars, academics, and other interested third parties who wish to study the Wikimedia Sites. Sharing this information helps them understand usage, viewing, and demographics statistics and patterns. They then can share their findings with us and our users so that we can all better understand and improve the Wikimedia Sites.

When we give access to personal information to third-party developers or researchers, we put requirements, such as reasonable technical and contractual protections, in place to help ensure that these service providers treat your information consistently with the principles of this Policy and in accordance with our instructions. If these developers or researchers later publish their work or findings, we ask that they not disclose your personal information. Please note that, despite the obligations we impose on developers and researchers, we cannot guarantee that they will abide by our agreement, nor do we guarantee that we will regularly screen or audit their projects. (You can learn more about re-identification in our FAQ.)

Back to top

Because You Made It Public

Information that you post is public and can been seen and used by everyone.

Any information you post publicly on the Wikimedia Sites is just that – public. For example, if you put your mailing address on your talk page, that is public, and not protected by this Policy. And if you edit without registering or logging into your account, your IP address will be seen publicly. Please think carefully about your desired level of anonymity before you disclose personal information on your user page or elsewhere.

Back to top



Protection

How Do We Protect Your Data?

We use a variety of physical and technical measures, policies, and procedures to help protect your information from unauthorized access, use, or disclosure.

We strive to protect your information from unauthorized access, use, or disclosure. We use a variety of physical and technical measures, policies, and procedures (such as access control procedures, network firewalls, and physical security) designed to protect our systems and your personal information. Unfortunately, there's no such thing as completely secure data transmission or storage, so we can't guarantee that our security will not be breached (by technical measures or through violation of our policies and procedures).

Back to top

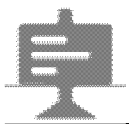
How Long Do We Keep Your Data?

We only keep your personal information as long as necessary to maintain, understand, and improve the Wikimedia Sites or to comply with U.S. law.

Once we receive personal information from you, we keep it for the shortest possible time that is consistent with the maintenance, understanding, and improvement of the Wikimedia Sites, and our obligations under applicable U.S. law. Non-personal information may be retained indefinitely. (Check out the list of examples in our FAQ.)

Please remember that certain information is retained and displayed indefinitely, such as your IP address (if you edit while not logged in) and any public contributions to the Wikimedia Sites.

Back to top



Important info

For the protection of the Wikimedia Foundation and other users, if you do not agree with this Privacy Policy, you may not use the Wikimedia Sites.

Where is the Foundation & What Does That Mean for Me?

You are consenting to the use of your information in the U.S. and to the transfer of that information to other countries in connection to providing our services to you and others.

The Wikimedia Foundation is a non-profit organization based in San Francisco, California, with servers and data centers located in the U.S. If you decide to use Wikimedia Sites, whether from inside or outside of the U.S., you

consent to the collection, transfer, storage, processing, disclosure, and other uses of your information in the U.S. as described in this Privacy Policy. You also consent to the transfer of your information by us from the U.S. to other countries, which may have different or less stringent data protection laws than your country, in connection with providing services to you.

Back to top

Our Response to Do Not Track (DNT) signals

We do not allow tracking by third-party websites you have not visited.

We do not share your data with third parties for marketing purposes.

We are strongly committed to not sharing nonpublic information with third parties. In particular, we do not allow tracking by third-party websites you have not visited (including analytics services, advertising networks, and social platforms), nor do we share your information with any third parties for marketing purposes. Under this Policy, we may share your information only under particular situations, which you can learn more about in the "When May We Share Your Information" section of this Privacy Policy.

Because we protect all users in this manner, we do not change our behavior in response to a web browser's "do not track" signal.

For more information regarding Do Not Track signals and how we handle them, please visit our FAQ.

Back to top

Changes to This Privacy Policy

Substantial changes to this Policy will not be made until after a public comment period of at least 30 days.

Because things naturally change over time and we want to ensure our Privacy Policy accurately reflects our practices and the law, it may be necessary to modify this Privacy Policy from time to time. We reserve the right to do so in the following manner:

- In the event of substantial changes, we will provide the proposed changes to our users in at least three (3) languages (selected at our discretion) for open comment period lasting at least thirty (30) calendar days. Prior to the start of any comment period, we will provide notice of such changes and the opportunity to comment via the Wikimedia Sites, and via a notification on WikimediaAnnounce-L or a similar mailing list.
- For minor changes, such as grammatical fixes, administrative or legal changes, or corrections of inaccurate statements, we will post the changes and, when possible, provide at least three (3) calendar days' prior notice via WikimediaAnnounce-L or similar mailing list.

We ask that you please review the most up-to-date version of our Privacy Policy. Your continued use of the Wikimedia Sites after this Privacy Policy becomes effective constitutes acceptance of this Privacy Policy on your part. Your continued use of the Wikimedia Sites after any subsequent version of this Privacy Policy becomes effective, following notice as outlined above, constitutes acceptance of that version of the Privacy Policy on your part.

Contact Us

If you have questions or suggestions about this Privacy Policy, or the information collected under this Privacy Policy, please email us at privacy@wikimedia.org (mailto:privacy@wikimedia.org) or contact us directly.

Thank You!

Thank you for reading our Privacy Policy. We hope you enjoy using the Wikimedia Sites and appreciate your participation in creating, maintaining, and constantly working to improve the largest repository of free knowledge in the world.

This privacy policy was approved by the board on April 25th 2014 and went into effect on June 6, 2014. Previous versions can be found below:

- **Privacy policy (November 2008 - June 2014): effective from November 25, 2008 until June 6, 2014**

- **Privacy policy (August 2008 - November 2008): effective from August 19, 2008 until November 25, 2008.**
- **Privacy policy (June 2006 - August 2008): effective from June 21, 2006 until August 19, 2008.**
- **Privacy policy (April 2005 to June 2006): effective from April 2005 until June 21, 2006**

Please note that in the event of any differences in meaning or interpretation between the original English version of this Privacy Policy and a translation, the original English version takes precedence.

Back to top

± (https://wikimediafoundation.org/w/index.php?title=Template:Privacy_policy_navigation_2&action=edit)

Privacy-related pages

Privacy policy · FAQ · Glossary of key terms · Wikimedia blog privacy policy · Subpoena FAQ · Access to nonpublic information · Data retention guidelines · Donor policy · Requests for user information

Retrieved from "https://wikimediafoundation.org/w/index.php?title=Privacy_policy&oldid=113231"

This page was last edited on 14 February 2018, at 22:37.

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 36

OPERATIONS, TECHNOLOGY

The future of HTTPS on Wikimedia projects

By Ryan Lane
August 1st, 2013

The Wikimedia Foundation believes strongly in protecting the privacy of its readers and editors. Recent leaks of the NSA's XKeyscore program have prompted our community members to push for the use of HTTPS by default for the Wikimedia projects. Thankfully, this is already a project that was being considered for this year's official roadmap and it has been on our unofficial roadmap since native HTTPS was enabled. Our current architecture cannot handle HTTPS by default, but we've been incrementally making changes to make it possible. Since we appear to be specifically targeted by XKeyscore, we'll be speeding up these efforts.

THIS ARTICLE IS AVAILABLE IN:

ENGLISH 中文

The Wikimedia Foundation believes strongly in protecting the privacy of its readers and editors. Recent leaks of the NSA's XKeyscore program have prompted our community members to push for the use of HTTPS by default for the Wikimedia projects. Thankfully, this is already a project that was being considered for this year's official roadmap and it has been on our unofficial roadmap since native HTTPS was enabled.

Our current architecture cannot handle HTTPS by default, but we've been incrementally making changes to make it possible. Since we appear to be specifically targeted by XKeyscore, we'll be speeding up these efforts. Here's our current internal roadmap:

1. Redirect to HTTPS for log-in, and keep logged-in users on HTTPS. ~~This change is scheduled to be deployed on August 21, at 16:00 UTC.~~ **Update as of 21 August**: we have delayed this change and will now deploy it on Wednesday, August 28 at 20:00 UTC/1pm PT.
2. Expand the HTTPS infrastructure: Move the SSL terminators directly onto the frontend varnish caches, and expand the frontend caching clusters as necessitated by increased load.
3. Put in engineering effort to more properly distribute our SSL load across the frontend caches. In our current architecture, we're using a source hashing based load balancer to allow for SSL session resumption. We'll switch to an SSL terminator that supports a distributed SSL cache, or we'll add one to our current solution. Doing so will allow us to switch to a weighted round-robin load balancer and will result in a more efficient SSL cache.
4. Starting with smaller projects, slowly soft-enable HTTPS for anonymous users by default, gradually moving toward soft-enabling it on the larger projects as well. By soft-enable we mean changing our rel=canonical links in the head section of our pages to point to the HTTPS version of pages, rather than the HTTP versions. This will cause search engines to return HTTPS results, rather than HTTP results.

GET CONNECTED

GET OUR EMAIL UPDATES

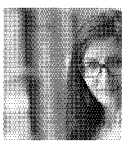
Your email address

Subscribe

MEET OUR COMMUNITY



The one-man band writing the history of Nigerian cinema into Wikipedia



Wikipedia is a to "plant and harvest" free knowledge: Ar Aghayan

More Community Profiles

MOST VIEWED THIS MONTH

'Monumental' winners from th world's largest photo contest showcase history and heritage

The top fifteen images from Wiki...

Türkiye'den Vikipedi'ye erişim engeli halen devam ediyor

Vikipedi'nin tüm dil sürümleri, Nisan ayını

New monthly dataset shows w people fall into Wikipedia rabl holes

The Wikimedia Foundation's Analytics te

ARCHIVES

FEBRUARY 2018

JANUARY 2018

5. Consider enabling perfect forward secrecy. Enabling perfect forward secrecy is only useful if we also eliminate the threat of traffic analysis of HTTPS, which can be used to detect a user's browsing activity, even when using HTTPS.
6. Consider doing a hard-enable of HTTPS. By hard-enable we mean force redirecting users from HTTP pages to the HTTPS versions of those pages. A number of countries, China being the largest example, completely block HTTPS to Wikimedia projects, so doing a hard-enable of HTTPS would probably block large numbers of users from accessing our projects at all. Because of this, we feel this action would probably do more harm than good, but we'll continue to evaluate our options here.
7. Consider enabling HTTP Strict Transport Security (HSTS) to protect against SSL-stripping man-in-the-middle attacks. Implementing HSTS could also lead to our projects being inaccessible for large numbers of users as it forces a browser to use HTTPS. If a country blocks HTTPS, then every user in the country that received an HSTS header would effectively be blocked from the projects.

Currently we don't have time frames associated with any change other than redirecting logged-in users to HTTPS, but we will be making time frames internally and will update this post at that point.

Until HTTPS is enabled by default, we urge privacy-conscious users to use HTTPS Everywhere or Tor [1].

Ryan Lane
Operations Engineer, Wikimedia Foundation

[1]: There are restrictions with Tor; see Wikipedia's information on this.

50 Comments on The future of HTTPS on Wikimedia projects

zzo38 3 years

Can you ***PLEASE*** add another domain name that disables HTTPS? I want to opt-out of HTTPS and I can no longer do so.

Share

peter 3 years

Are you kidding Wikimedia?

"Consider doing a hard-enable of HTTPS. By hard-enable we mean force redirecting users from HTTP pages to the HTTPS versions of those pages. A number of countries, China being the largest example, completely block HTTPS to Wikimedia projects, so doing a hard-enable of HTTPS would probably block large numbers of users from accessing our projects at all. Because of this, we feel this action would probably do more harm than good, but we'll continue to evaluate our options here."

Because Chinese government is raping the Internet in China you do not enable HTTPS as hard-enable? Are you getting payed from Chinese government? Are you technicians that stupid? What is the reason to not hard-enable it? Because other people are doing bad things you do not the good? WTF?

Share

John Gilmore 4 years

Isn't it interesting how the Chinese government and NSA BOTH spy on users of Wikipedia?

I think Chinese users of Wikipedia should blame their government — not Wikipedia — for any problems that result from Wikipedia moving to encrypt more and more of their service. Wikipedia is solving a problem. The Chinese government is creating one.

DECEMBER 2017
NOVEMBER 2017
OCTOBER 2017
OLDER POSTS 26

WORK AT WIKIMEDIA

Work with the foundation that supports W and its sister projects around the world. A and join us

It's too much to expect that the entire world should use Wikipedia in plaintext, letting any government or criminal spy on all the users, because a few governments infringe their citizens' right to use encryption. US citizens actively fought the US government's ban on encryption — and won, after a decade of work. Chinese citizens, it's your turn to fix your own government now. The rest of the world can't do it for you.

Share

KoshVorlon 4 years

* FOR ALL THOSE THAT WANT TO FLAME THE DEVS OVER THIS *

Yes – this change breaks Mozilla – it's already known.
I.E and Chrome still handles the change over fine.

You may need to switch over if your a firefox user (as I am).

Flaming the devs won't get this fixed faster.

Share

Ryan Lane 4 years

We have plans on testing SPDY after anonymous users are switched to HTTPS.

Share

Leirn 4 years

Will SPDY be next ?

Share

Ryan Lane 4 years

There wasn't any claim that adding HTTPS would completely alleviate our woes in this regard. This is only a first step towards the goal.

Share

Seb35 4 years

I want just to point that the History of cryptography should teach us to never over-expect the attacker don't have advanced techniques to cryptanalyse or decipher our message with some means (see the period where the cipher was the secret, or Enigma, Purple, recent attacks on TLS; even one-time pads can be broken if the key is not truly random). In this sense I find we should not claim "our infrastructure is secure and TLS is not a false sense of security" but "to the best of our knowledge, access to Wikimedia projects through TLS is secure regarding most of the currently known attacks".

Share

wiiliam gomes 5 years

éu gosto de asistir é irado

Share

Nicolas B. 5 years

Ryan,

Alas, Wikipedia blocks contributions from many proxies, and from TOR.

Ranyv,

Chinese people ≠ people in China.

Share

Int21h 5 years

Leave the Zhongwen Wikipedia behind. Let them keep their HTTP.

Advance the rest of the world into the 20th Century.

Share

300aq300aq 5 years

坚决支持！！！！！！！！！！

Share

qa003qa003 5 years

坚决反对！！！！！！！！！！

Share

Ryan Lane 5 years

So, HTTPS forces them to do traffic analysis, which makes their lives quite a bit harder. So, it's not a false sense of security, but isn't by itself a complete solution. As mentioned, newer protocols will likely help this situation, but we'll also be putting effort into making traffic analysis more difficult for our traffic. Our first priority, of course, is moving people to HTTPS.

Share

Ciara Hoyle 5 years

So much for clarity! That should read the above comment #10

Share

Ciara Hoyle 5 years

For clarity – the above comment #9, is a follow-on from my previous comment #2 on page 2

Share

Ciara Hoyle 5 years

Very interesting. Seeing as we are talking about eavesdropping by those with the resources a nation state (NSA et al.) doesn't the finger printing by traffic analysis issue also compromise the perceived privacy provided by 'vanilla' HTTPS? If so, are the measures described in the blog really just giving ourselves a false sense of privacy (regarding NSA level eavesdropping)?

Share

Walter Grassroot@zhwiki 5 years

As a 5-year Wikipedia editor, I appreciate for WMF's efforts on every promotion, including security protection. However, this attempt of moving to HTTPS on Wikimedia projects will completely destroy the Chinese community to reach all the Wikimedia programs, not only Zh-wikipedia. Since 2008, our Chinese Wikipedia has suffered governmental blocks for different reasons. Although we could access the HTTPS early 2013, the government still blocked this method to reach Wikipedia immediately, when we recommended this in public. Many Wikipedia-unfriendly governments would learn and act same as the Chinese Government on internet control – which means, if WMF act HTTPS on whole Wikimedia projects, more editors will suffered the block reflection in the world. In general, this action would setup all the Wikipedians in the opposite side of the governments. Thank you.

Share

Jsjsjs1111 5 years

Even if this "feature" is brought into practice, I would still strongly recommend you not to enable it on Chinese Wikipedia (zh), as for the reason that Quark stated. You are free to enable it elsewhere.

Share

Ryan Lane 5 years

Matt: China blocks Wikimedia projects on HTTPS currently, yes.

Share

MORE COMMENTS

Comments are closed.

WIKIMEDIA FOUNDATION

The Wikimedia Foundation, Inc is a nonprofit charitable organization dedicated to encouraging the growth, development and distribution of free, multilingual content, and to providing the full content of these wiki-based projects to the public free of charge. Get Involved | Log In

WIKIMEDIA PROJECTS

The Wikimedia Foundation operates some of the largest collaboratively edited reference projects in the world.

WIKIPEDIA COMMONS MEDIAWIKI WIKIBOOKS
WIKIDATA WIKINEWS WIKIQUOTE WIKISOURCE
WIKISPECIES WIKIVERSITY WIKIVOYAGE WIKTIONARY

WIKIMEDIA MOVEMENT AFFILIATES

The Wikimedia projects have an international scope, and the Wikimedia movement ha already made a significant impact throughout the world. To continue this success on a organizational level, Wikimedia is building an international network of associated organizations.

WIKIMEDIA CHAPTERS THEMATIC ORGANIZATIONS WIKIMEDIA USER GROUPS

This work is licensed under a Creative Commons Attribution 3.0 unported license. Some images under CC BY-SA.
Read our Terms of Use and Privacy policy. | Powered by WordPress.com VIP

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

Plaintiff's Exhibit 37

Photo by Colin, CC-E

FOUNDATION, LEGAL, PLATFORM ENGINEERING, TECHNOLOGY, WIKIPEDIA

Securing access to Wikimedia sites with HTTPS

By Yana Welinder
Victoria Baranetsky, Wikimedia Foundation
Brandon Black, Wikimedia Foundation
June 12th, 2015

The Wikimedia Foundation is happy to announce that we are implementing HTTPS to encrypt all traffic on Wikimedia sites. With this change, nearly half a billion monthly visitors on Wikipedia and its sister projects will be able to share in the world's knowledge more securely.

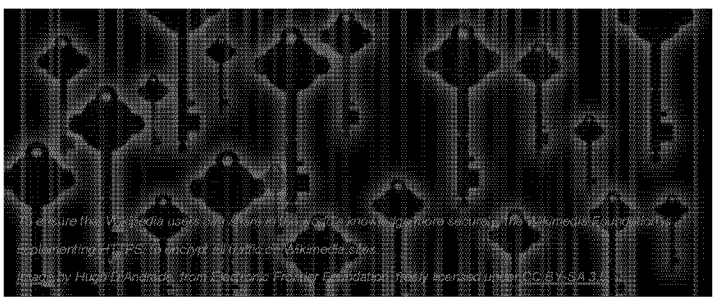


Image by Hugo D'Andrade, from Flickr, Premier Exhibition, freely licensed under C.C.B.Y.S.A.3.0

To be truly free, access to knowledge must be secure and uncensored. At the Wikimedia Foundation, we believe that you should be able to use Wikipedia and the Wikimedia sites without sacrificing privacy or safety.

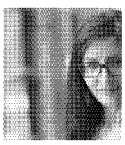
Today, we're happy to announce that we are in the process of implementing HTTPS to encrypt all Wikimedia traffic. We will also use HTTP Strict Transport Security (HSTS) to protect against efforts to 'break' HTTPS and intercept traffic. With this change, the nearly half a billion people who rely on Wikipedia and its sister projects every month will be able to share in the world's knowledge more securely.

The HTTPS protocol creates an encrypted connection between your computer and Wikimedia sites to ensure the security and integrity of data you transmit. Encryption makes it more difficult for governments and other third parties to monitor your traffic. It also makes it harder for Internet Service Providers (ISPs) to censor access to specific Wikipedia articles and other information.

HTTPS is not new to Wikimedia sites. Since 2011, we have been working on establishing the infrastructure and technical requirements, and understanding the policy and community implications of HTTPS for all Wikimedia traffic, with the ultimate goal of making it available to all users. In fact, for the past four years, Wikimedia users could access our sites with HTTPS manually, through HTTPS Everywhere, and when directed to our sites from major search engines. Additionally, all logged in users have been accessing via HTTPS since 2013.



The one-man band writing the history of Nigerian cinema into Wikipedia



Wikipedia is a to "plant and harvest" free knowledge: Ar Aghayan

'Monumental' winners from th world's largest photo contest showcase history and heritage

The top fifteen images from Wiki...

Türkiye'den Vikipedi'ye erişim engeli halen devam ediyor

Vikipedi'nin tüm dil sürümleri, Nisan ayını

New monthly dataset shows w people fall into Wikipedia rabl holes

The Wikimedia Foundation's Analytics te

Over the last few years, increasing concerns about government surveillance prompted members of the Wikimedia community to push for more broad protection through HTTPS. We agreed, and made this transition a priority for our policy and engineering teams.

We believe encryption makes the web stronger for everyone. In a world where mass surveillance has become a serious threat to intellectual freedom, secure connections are essential for protecting users around the world. Without encryption, governments can more easily surveil sensitive information, creating a chilling effect, and deterring participation, or in extreme cases they can isolate or discipline citizens. Accounts may also be hijacked, pages may be censored, other security flaws could expose sensitive user information and communications. Because of these circumstances, we believe that the time for HTTPS for all Wikimedia traffic is now. We encourage others to join us as we move forward with this commitment.

The technical challenges of migrating to HTTPS

HTTPS migration for one of the world's most popular websites can be complicated. For us, this process began years ago and involved teams from across the Wikimedia Foundation. Our engineering team has been driving this transition, working hard to improve our sites' HTTPS performance, prepare our infrastructure to handle the transition, and ultimately manage the implementation.

Our first steps involved improving our infrastructure and code base so we could support HTTPS. We also significantly expanded and updated our server hardware. Since we don't employ third party content delivery systems, we had to manage this process for our entire infrastructure stack in-house.

HTTPS may also have performance implications for users, particularly our many users accessing Wikimedia sites from countries or networks with poor technical infrastructure. We've been carefully calibrating our HTTPS configuration to minimize negative impacts related to latency, page load times, and user experience. This was an iterative process that relied on industry standards, a large amount of testing, and our own experience running the Wikimedia sites.

Throughout this process, we have carefully considered how HTTPS affects all of our users. People around the world access Wikimedia sites from a diversity of devices, with varying levels of connectivity and freedom of information. Although we have optimized the experience as much as possible with this challenge in mind, this change could affect access for some Wikimedia traffic in certain parts of the world.

In the last year leading up to this roll-out, we've ramped up our testing and optimization efforts to make sure our sites and infrastructure can support this migration. Our focus is now on completing the implementation of HTTPS and HSTS for all Wikimedia sites. We look forward to sharing a more detailed account of this unique engineering accomplishment once we're through the full transition.

Today, we are happy to start the final steps of this transition, and we expect completion within a couple of weeks.

Yana Welinder, Senior Legal Counsel, Wikimedia Foundation
Victoria Baranetsky, Legal Counsel, Wikimedia Foundation
Brandon Black, Operations Engineer, Wikimedia Foundation

40 Comments on Securing access to Wikimedia sites with HTTPS

Uityyy 7 months

How do I manually force unencrypted access on an old mobile browser that does not support HTTPS?
I have one that 's failing to access en.m.wikipedia.org, apparently because of this, and I see no solution here.
Any magic "en.insecure.wikipedia.org"?

Share

DECEMBER 2017
NOVEMBER 2017
OCTOBER 2017
OLDER POSTS 26

WORK AT WIKIMEDIA

Work with the foundation that supports W and its sister projects around the world. A and join us

Frushi 8 months

HTTPS is a 'must have' in present internet. When Google said it's gonna take a closer look for a website that don't use SSL it become clear that even websites which don't need them (because they don't have any secure infomation) will have to go to HTTPS from old http.

Share

Tom 1 year

Following the huge fail of the french ISP Orange redirecting wikipedia.fr and others, why wikipedia.fr is not protect with https/HSTS ?
http://www.theregister.co.uk/2016/10/18/orange_blows_up_french_gov_website/

Share

bart 1 year

Google usually has an alternate (cache) for each wiki link.
I just use these cache pages.

Share

Rodion 2 years

I also want there is a way to use wikipedia with plain HTTP if necessary. Currently there is a stupid debate between our government and local wiki representatives (I could not decide which of them is more stupid, I'm sorry) about restricting access to certain pages (about drugs). Providers can do this for single page if it is accessed with HTTP, but they need to deny access to whole website if it is accessed via HTTPS.

So it would be good if we have some fallback, perhaps with banner explaining "all horrible consequences" of reading wiki in plain HTTP. In my personal opinion being super-obsessed with security measures may sometimes create unwanted problems to other people :(

Share

Creg 3 years

Flo said

"Concerning privacy: when you browse Wikipedia the URLs contain the topic you are reading thus any sniffer can track what you are currenly reading. Only the *contents* is encrypted, but the contents is visible by anybody anyway (in contrast to the content of my bank account)."

False. The root domain (wikipedia.org) can be inferred from the IP address of the server during the TCP/IP request but the complete URL and exact page you're reading cannot.

Read the article on https.

Share

Flo 3 years

Is there *any* way to use Wikipedia *without* https?
I have an old device which is not capable of using https. And please don't tell me to buy new hardware or software.
So please offer a possibility to read Wikipedia *without* forced https!!!!

BTW: I cannot follow the reasons to *enforce* https:
Concerning privacy: when you browse Wikipedia the URLs contain the topic you are reading (e.g.:

https://en.wikipedia.org/wiki/CMAC) thus any sniffer can track what you are currenly reading. Only the *contents* is encrypted, but the contents is visible by anybody anyway (in contrast to the content of my bank account).

Concerning "integrity of data": nobody will guarantee that the content of Wikipedia is accurate because everybody can contribute to it. Thus I do not *fully* rely to anything I read in Wikipedia.

Share

omtim 3 years

Great step for sure, actually, in digital world https is more imperative

Share

Gary Smith 3 years

All the points are explained very clearly, Great source of information. Thanks for en-lighting us with your knowledge, it is helpful for many of us.

Share

Sports Fan Stan 3 years

All well and good to force everyone to use https. Would it be too much to ask to employ a real SSL certificate that doesn't rely on a wildcard. At present, we can't even use Wikipedia anymore because we can't trust the website. Uggghhh…

Share

astrodevamm 3 years

Very good step indeed, in fact, in cyber world https is more important because of security issues. Know a days users check website also they check that website https not. If they found https is not they click on cut button and skip from website…

Share

Pushpendra Pal 3 years

Great move team. Web is becoming a tool for governments and enforcement agencies to surveillance on citizens. SSL helps website visitors to send and receive encrypted data.

I also want to move my website http://careervendor.com from HTTP to HTTPS. I am fearing about loosing traffic, backlink and ranking. Can anyone please suggest a way for proper migration.

Share

astrodevamm 3 years

Very good step indeed, in fact, in cyber world https is more important because of security issues. Know a days users check website also they check that website https not. If they found https is not they click on cut button and skip from website…

Share

Ron 3 years

> There are two reasons someone might ask for any form of downgrade or opt-out to be permitted:

Make that three reasons.
I run in DOS, and I like to keep the functionality of Arachne.

Yes, I also run Links, Elinks and Lynx in DOS, but Arachne is more versatile than all of them – except for a lack of SSL.

Share

zzo38 3 years

I *really* want the ability to connect without HTTPS. I want to avoid the overhead required by HTTPS please.

Share

Mat2 3 years

"Because then a man in the middle can replace anyone's user agent details with another user agent, and bingo, nobody any longer has any encryption at all. Invisibly and undetectably."
Such an attack is already possible with tools such as sslstrip. Therefore user-agent sniffing doesn't decrease security for other users out there: it will make life easier neither for criminals nor for companies that want to monitor traffic.
Wikipedia is going to use HSTS and add itself to HSTS preload lists in browsers: that will block downgrade to HTTP for new browsers.

"Upgrading from IE6 to a secure browser is entirely possible for every single user on the planet. There is no sane reason for anyone, anywhere, to use an insecure browser."
Not every computer user can do this, unfortunately.

Google makes sure that IE6 still works:
https://www.ssllabs.com/ssltest/analyze.html?d=google.com&s=74.125.239.96&hideResults=on
Wikipedia is such an important site on the internet.

Share

dewimorgan 3 years

"Wouldn't it be possible to add some user-agent sniffing" NO! No it would not. Because then a man in the middle can replace anyone's user agent details with another user agent, and bingo, nobody any longer has any encryption at all. Invisibly and undetectably. Why would wikimedia hand attackers such a gift on a plate?

Upgrading from IE6 to a secure browser is entirely possible for every single user on the planet. There is no sane reason for anyone, anywhere, to use an insecure browser. The very worst smartphone and smartwatch in the world can browse securely. Even Lynx can handle secure browsing, and that's been ported to just about everything.

There are two reasons someone might ask for any form of downgrade or opt-out to be permitted: 1) they are grievously uninformed; or 2) they are maliciously requesting the downgrade on behalf of some organization which wants a MitM attack to work.

One wonders how many of each group is commenting here.

Share

Mat2 3 years

Now all IE6 users will be cut off from using Wikipedia:
https://www.ssllabs.com/ssltest/analyze.html?d=en.wikipedia.org

Wouldn't it be possible to add some user-agent sniffing so that these browsers could still access Wikipedia? They are usually used by poorer people.

Share

Ron Clarke 3 years

Steve,
> Why now adding a SSL/TLS support to that browser instead, is this really something very hard to do, or just not a priority?

Adding SSL to Arachne would be wonderful, and we wish we could. But.....we have a lack of suitably skilled coders with an interest in DOS browsers, and Arachne in particular.

Any volunteers ?

Share

dewimorgan 3 years

@Glenn McCorkle and Ron Clarke:

"Ron & I are active developers of DOS Arachne"

This ship has sailed.

Every single .gov domain will be HTTPS-only by next year. Many already are.

For active developers of web browsers which don't support HTTPS, implementing it should have been the number one priority for the last few years, because other browsers – even other command-line browsers that can run on legacy hardware – support it just fine. Like an FTP program without FTPS or SFTP, or an email program without STARTTLS, you'll lose market share and relevance.

Oh, and IPv6 URLs are a thing now, too.

Share

MORE COMMENTS

Comments are closed.

WIKIMEDIA FOUNDATION
The Wikimedia Foundation, Inc is a nonprofit charitable organization dedicated to encouraging the growth, development and distribution of free, multilingual content, and to providing the full content of these wiki-based projects to the public free of charge. Get Involved | Log In

WIKIMEDIA PROJECTS

The Wikimedia Foundation operates some of the largest collaboratively edited reference projects in the world.

WIKIPEDIA COMMONS MEDIAWIKI WIKIBOOKS
WIKIDATA WIKINEWS WIKIQUOTE WIKISOURCE
WIKISPECIES WIKIVERSITY WIKIVOYAGE WIKTIONARY

WIKIMEDIA MOVEMENT AFFILIATES

The Wikimedia projects have an international scope, and the Wikimedia movement ha already made a significant impact throughout the world. To continue this success on a organizational level, Wikimedia is building an international network of associated organizations.

WIKIMEDIA CHAPTERS THEMATIC ORGANIZATIONS WIKIMEDIA USER GROUPS

This work is licensed under a Creative Commons Attribution 3.0 unported license. Some images under CC BY-SA.
Read our Terms of Use and Privacy policy. | Powered by WordPress.com VIP

USCA4 Appeal: 20-1191 Doc: 18-5 Filed: 07/01/2020 Pg: 447 of 529

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

Plaintiff's Exhibit 38

From: Mark Bergsma
To: Faidon Liambotis
Sent: 5/23/2014 1:16:25 PM
Subject: Fwd: Ops Goals: Questions/Expectations

Begin forwarded message:

From: Erik Moeller <erik@wikimedia.org>
Subject: Ops Goals: Questions/Expectations
Date: 23 May 2014 10:19:54 GMT+2
To: Mark Bergsma <mark@wikimedia.org>

Hi Mark,

For the goalsetting process, I'm drafting a set of questions/expectations for each team. I'll share the whole document with EMGT later, but wanted to send you the ops piece upfront just so you can take a quick spin through it. Any quick reactions welcome :)

I'd like to publish this as a subpage to the goals page once it's gone through a first pass EMGT review. The intent of this is to spur some specific thinking, but also get on the same page on the things we feel we must accomplish in the coming year. You can have conversations about this with me, with your team, or with others in the org, as you see fit.

Erik

Site Operations

Questions

- Will we be able to achieve full failover capability from EQIAD to CODFW? Should we set a goal such as quarterly failover tests? (How do we avoid a situation like with TPA where we lost failover capability?) What's the plan for CODFW utilization beyond as a secondary?
- Can we articulate goals related to use of virtualization in our infrastructure beyond Labs?
- Do we intend to plan out any additional caching location(s)? If so, can we articulate expected user benefit?
- Do we intended to implement off-site backups beyond cross-DC copies? If so, when?
- Can we establish some metrics for ongoing high-level reporting (uptime/outages/latency by service/geography etc.)?

Expectations

- 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 PFS
  - enabling IPSEC
  - investigating techniques to defeat traffic detection
  - making a definitive decision on whether to force HTTPS for all users.

  Let's try to attach a rough timetable to relevant objectives.

Wikimedia Labs

Questions

- What additional data/computing resources/services should we aim to make available to the Labs community? How can we accomplish that (are there cross-functional dependencies, e.g. with analytics)?
- What infrastructure improvements are going to get us the largest bang for the buck in terms of stability/performance improvements?
- Are there needs by other teams (e.g. release engineering) that aren't currently met effectively with the Labs infrastructure? (Example: improved automatic provisioning of Labs VMs for parallelized unit test execution - multiple changesets/branches). If so, how should these needs be met? If not, how do we minimize wheel-reinvention by other teams?
- How can we more consistently showcase awesome Labs community innovations? Are there better ways to interface with the grantmaking team to ensure volunteers receive financial support as appropriate?

Expectations

- I would like us to begin articulating a more compelling vision for the lifecycle of community innovations. We've improved on the toolserver situation, but we could still do better along the following dimensions:
  - discoverability of tools
  - integration of tools into the main site experience
  - better support for Labs->Production migration where appropriate

  We may not be able to resource a more comprehensive "Labs vision" yet, but we should at least begin articulating it and defining the steps we would need to take to get there (e.g. form a cross-functional team incuding MW core/API & UX expertise).
- Let's think about two staffing scenarios: 1) serving the core Labs purpose well, 2) raising the bar and creating a larger vision for Labs consistent with the above. What would those scenarios translate to in terms of additional FTEs and their skillsets? If the ideal Labs team is a cross-functional one, let's start having that conversation.

--
Erik Möller
VP of Engineering and Product Development, Wikimedia Foundation

—
Mark Bergsma <mark@wikimedia.org>
Lead Operations Architect
Director of Technical Operations
Wikimedia Foundation

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY FOIA Confidential Treatment Request~~

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

Plaintiff's Exhibit 39

Maniphest > T81543 Create Task

Enable IPSec between datacenters

Closed, Resolved Public

Description

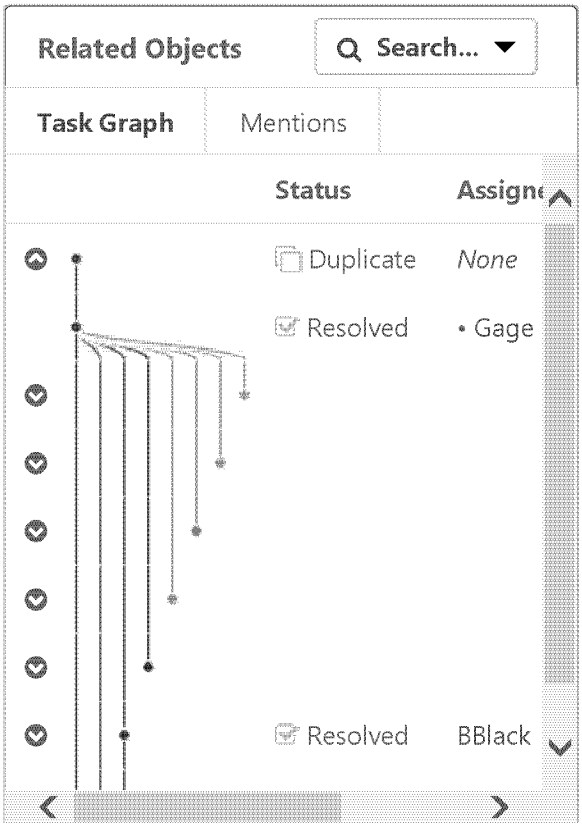
Traffic between our datacenters goes across fibers that are potentially surveilled. Since we terminate HTTPS immediately at the first hop, this means that user traffic gets across to the main datacenter in cleartext.

Details

Reference rt3536

Related Objects Search...

Task Graph | Mentions



Tags

Interdatacenter-IPsec
Traffic (Done)
Operations

Subscribers

Matanya, faidon, greg and 9 others

Tokens

Assigned To

• **Gage**

Authored By

• **rtimport**, Sep 11 2012



• **rtimport** added a project: ~~**ops-core**~~. Dec 18 2014, 1:23 AM

• **rtimport** raised the priority of this task from to *Normal*.

• **rtimport** set Reference to rt3536.

• **rtimport** created this task.
Sep 11 2012, 5:20 PM

faidon added a comment.
Sep 11 2012, 9:07 PM

On Tue, Sep 11, 2012 at 05:20:36PM +0000, Ryan Lane via RT wrote:

> *Traffic between esams and the US datacenters goes across the WAN. This means HTTPS isn't actually encrypted for esams users. Also, we're sending IP information across the WAN, which is privacy information.*

Having IPsec tunnels between esams and the US means we're going to have a lower MTU which is going to be a constant PITA. IPsec is also hard and difficult to debug. I'd much prefer doing something like

stunnel or
pound and use plain ol' HTTPS.
Regards,
Faidon

• **rtimport** added a comment.
Sep 11 2012, 9:07 PM

Status changed from 'new' to 'open' by RT_System

tstarling added a comment.
Jul 8 2013, 11:29 PM

For users geolocated in Europe, HTTPS connections are terminated in esams and then the requests are forwarded unencrypted to eqiad. 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.

mark added a comment.
Jul 9 2013, 8:46 AM

On Mon Jul 08 23:29:10 2013, tstarling wrote:

> *For users geolocated in Europe, HTTPS connections are terminated in esams and then the requests are forwarded unencrypted to eqiad. 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.*

Not just esams. Any link that leaves our data centers is equally suspect. So
that also includes pmtpa vs eqiad, and soon ulsfo.
Dedicated ipsec hardware is not very practical for this, and also pretty
expensive. But I'd like to experiment with ipsec host-to-host (which is really
what it was meant for) at some point...

--
Mark Bergsma <mark at wikimedia>
Lead Operations Architect
Wikimedia Foundation

• **rtimport** added a comment.
Jul 9 2013, 8:46 AM

Status changed from 'new' to 'open' by RT_System

mark added a comment.
Jul 9 2013, 8:46 AM

Queue changed from procurement to core-ops by mark

mark added a comment.
Jul 9 2013, 9:06 AM

On Tue Jul 09 08:46:08 2013, mark wrote:

> *Dedicated ipsec hardware is not very practical for this, and also pretty expensive. But I'd like to experiment with ipsec host-to-host (which is really what it was meant for) at some point...*

I'd like to (re)try IPsec in Linux with ESP in "transport mode".

The advantage
here is that this doesn't need any routing changes, and avoids the significant
complication of rerouting (all) traffic between these hosts with separate
(policy) routing, which tends to break things for traffic that is not supposed
to use the tunnel/VPN. In transport mode we can select exactly which traffic
(payload only) we want to encrypt, and not the rest.
We're already getting MPLS transport to esams to avoid some of this, but that
doesn't (really) solve the encryption problem. If ESP in transport mode works
well, that would solve it in a scaleable way. Fortunately we have sufficient
configuration management in place that maintaining such a setup across many
hosts is no longer a problem.
With our MPLS links we'll be able to do Jumbo
frames, so we will even be able to support MTU 1500 and up with IPsec.
I've used IPsec with Linux about 10 years ago, and it had some problems then -
especially in a mixed environment with other vendors such as Cisco routers.
Rekey failures and negotiation problems. I'm hoping the

situation is better
now, especially in a uniform
Linux environment.
--
Mark Bergsma <mark at
wikimedia>
Lead Operations Architect
Wikimedia Foundation

faidon added a comment.
Jul 9 2013, 10:47 AM

On Tue, Jul 09, 2013 at
09:06:08AM +0000, Mark
Bergsma via RT wrote:

> *We're already getting MPLS transport to esams to avoid some of this,*
> *but that doesn't (really) solve the encryption problem. If ESP in*
> *transport mode works well, that would solve it in a scaleable way.*
> *Fortunately we have sufficient configuration management in place that maintaining such a setup across many hosts is no longer a problem. With our MPLS links we'll be able to do Jumbo frames, so we will even be*
> *able to support MTU 1500 and up with IPsec.*

I don't have access to the
contract but I asked Leslie
yesterday and she

said that our yet-to-be-established link will have an MTU of 1514.

> *I've used IPsec with Linux about 10 years ago, and it had some problems then - especially in a mixed environment with other vendors such as Cisco routers. Rekey failures and negotiation problems. I'm hoping the situation is better now, especially in a uniform Linux environment.*

I've tried to use it a few years back with Linux and it was incredibly
messy. The software might have improved since, but I still expect a full
dual-stack IPsec setup in transport mode between with two/three
datacenters to be non-obvious in many ways and possibly fragile.
An alternative would be to just do SSL, e.g. via stunnel. That also has
a number of complexities, though.
Personally, I'd much rather prefer encryption be transparent to the hosts and be handled entirely on the network equipment level.
Faidon

tstarling added a comment.

Jul 9 2013, 12:41 PM

On Tue Jul 09 08:46:08 2013, mark wrote:

> *Dedicated ipsec hardware is not very practical for this, and also pretty expensive. But I'd like to experiment with ipsec host-to-host (which is really what it was meant for) at some point...*

This ticket came out of an IRC discussion:
<TimStarling> LeslieCarr: any guess what the cost of said equipment would be?
my googling has not yet been successful
<LeslieCarr> memory fails me :(if you open a ticket we can get some quotes

mark added a comment.

Jul 9 2013, 12:55 PM

On Jul 9, 2013, at 12:47 PM, "Faidon Liambotis via RT" <core-ops at rt> :)
--
Mark Bergsma <mark at wikimedia>
Lead Operations Architect
Wikimedia Foundation

mark added a comment.
Jul 12 2013, 12:29 PM

Merged into ticket #3536 by mark

mark added a comment.
Jul 12 2013, 12:29 PM

Merged into ticket #3536 by mark

jeremyb added a comment.
Aug 26 2013, 12:43 AM

AdminCc jeremyb added by jeremyb

tstarling added a comment.
Sep 10 2013, 1:11 AM

I don't understand why the MTU is important for IPsec feasibility. If it's only
for internal traffic, then MTU discovery will be efficient and reliable, right?
If we're just talking about the small performance loss due to lower TCP window
size etc., then surely that is better dealt with on a separate ticket, independently of IPsec.

tstarling added a comment.

Nov 1 2013, 10:43 AM

http://www.washingtonpost.com/wo
security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html?hpid=z1
According to the a recent leak from Edward Snowden, the NSA has already been
using links between Google datacentres to collect private information in
plaintext, so it's not a big jump to imagine that they are doing it with us
too.

coren added a comment.

Nov 1 2013, 2:00 PM

On Tue Jul 09 08:55:07 2013, mark wrote:

> *How about we try Linux IPsec, since it doesn't cost anything and isn't much work either. If it still sucks today, we can still buy expensive boxes or use stunnel... :)*

I agree with Mark without hesitation here; the Linux ipsec

implementation is comparably robust to any hardware available, would be relatively simple to deploy thanks to configuration management and costs us little but time to deploy experimentally. Interestingly enough, I've used a simplified ipsec setup in the past where, since our endpoints were fixed, we simply used configuration management deployed keys (i.e.: no IKE) to great effect. With a bit of automation for key rotation, this meant rock-solid host to host IPsec with no dependency on networking or an externally maintained daemon to be stable -- at the cost of having to do key management ourselves (which we did through ssh). [in case you are curious, the use case included boxes deployed in networks presumed hostile and also integrated with TPM which should be unneeded in our case] The advantage of doing it this way is that there is no capital investment required, no routing changes needed at all, and only hosts pairs we deem necessary need use IPsec at all; it's easy to deploy and

experiment on a subset of hosts.

• **Gage** merged a task: Restricted Task.
Dec 18 2014, 6:51 PM

• **Gage** claimed this task.

• **Gage** added a subscriber: • **rtimport**.

faidon renamed this task from *Enable IPSec between esams and US datacenters* to *Enable IPSec between datacenters*.
Dec 22 2014, 9:40 AM

faidon updated the task description. **(Show Details)**

faidon raised the priority of this task from *Normal* to *High*.

faidon set Security to None.

Aklapper added a subscriber: **tstarling**. Dec 22 2014, 8:52 PM

• **Gage** added a comment.
Dec 24 2014, 3:45 PM

Decisions have been made to use:

- Host-to-host connections between Varnish nodes in cache sites and those in main colos
- Transport mode (ESP without AH): only the payload is encrypted;

IP/TCP headers are not authenticated
- Strongswan daemon for ISAKMP
- IKEv2 via reuse of Puppet client's SSL certs + keys
- Assumption: nodes will run Ubuntu 14.04

Current status:

- A test setup is running between (berkelium|curium).eqiad and (cp3001|cp3002).esams in transport mode
  - Manual configuration, derived from http://www.strongswan.transport/
  - Hosts are sending syslog events to Logstash
- Connection resilience tested: 10% packet loss in each direction on berkelium
  - sudo iptables -A OUTPUT -d cp3001.esams.wmnet -m statistic --mode random --probability 0.1 -j DROP
  - sudo iptables -A INPUT -s cp3001.esams.wmnet -m statistic --mode random --probability 0.1 -j DROP
  - 10MB/sec throughput over IPsec tests complete successfully: iperf -c

berkelium.eqiad.wmnet
-b 10M

- Puppet module under development in 'ipsec' project in Labs
  - https://gerrit.wikimedia.
  - puppetmaster: ipsec-pm.eqiad.wmflabs
  - module: ipsec-pm:/var/lib/git/operatio
  - 12.04 clients: (ipsec-c1|ipsec-c2).eqiad.wmflabs
  - 14.04 clients: (ipsec-c3|ipsec-c4).eqiad.wmflabs

Remaining tasks:

- Improve reusability of puppet module
  - Support Ubuntu 12.04 which has /etc/init.d/ipsec instead of /etc/init/strongswan.
  - Support Debian Jessie which has /etc/init.d/ipsec
  - remove varnish node assumtions so that it can be used between any two nodes
  - remove wmf-specific dependencies so that it may be used outside of the org
  - make it work in Labs
  - achieve better code/data separation

- remove dependency on role::cache::configuratio
- Specify connections by IP rather than hostname in order to support IPv4 + IPv6 (SAs must be configured for each)

- Possibly restrict encryption to Varnish traffic using configuration parameters leftsubnet/rightsubnet which allow port specification
- Consider application of IPsec to non-Varnish inter-colo traffic
- Possibly add corresponding firewall rules to enforce use of IPsec

Problem:

- Configuration requires at least one side of a connected pair of hosts to specify the remote hostname (and v4 + v6 IPs, for our purposes)
- This means that the config file template in the puppet module must enumerate remote hosts
- This information is not currently available via facter or hiera
- Therefore we need a way to query for that list of nodes and their IPs
- Inspired by modules/torrus/templates/v

from manifests/role/cache.pp

- However that does not have clean code/data separation, and v4 + v6 IPs are not included

Solution?:

- Store data in Hiera: hostname, IPv4 address, IPv6 address, site and cluster membership for at least Varnish nodes

Documentation under development (to be moved to Wikitech): https://office.wikimedia.org/wiki/Use (WMF)/IPsec

mark added subscribers:

- **Gage**, **mark**.

Dec 29 2014, 1:47 PM

> In ~~**T81543#943073**~~,
> ○ **@Gage** wrote:
>
> *Decisions have been made to use:*
>
> - *Host-to-host connections between Varnish nodes in cache sites and those in main colos*
> - *Transport mode (ESP without AH): only the payload is encrypted; IP/TCP headers are not authenticated*

- *Strongswan daemon for ISAKMP*
- *IKEv2 via reuse of Puppet client's SSL certs + keys*
- *Assumption: nodes will run Ubuntu 14.04*

Current status:

- *A test setup is running between (berkelium|curium).eqiad and (cp3001|cp3002).esams in transport mode*
  - *Manual configuration, derived from http://www.strongswa transport/*
  - *Hosts are sending syslog events to Logstash*
- *Connection resilience tested: 10% packet loss in each direction on berkelium*
  - *sudo iptables -A OUTPUT -d cp3001.esams.wmnet -m statistic --mode random --probability 0.1 -j DROP*
  - *sudo iptables -A INPUT -s cp3001.esams.wmnet -m statistic --mode random --probability 0.1 -j*

> - *10MB/sec throughput over IPsec tests complete successfully: iperf -c berkelium.eqiad.wmn -b 10M*

Thanks, this is very helpful!

> *Remaining tasks:*
>
> - *Improve reusability of puppet module*
>   - *Support Ubuntu 12.04 which has /etc/init.d/ipsec instead of /etc/init/strongswa*
>   - *Support Debian Jessie which has /etc/init.d/ipsec*
>   - *remove varnish node assumtions so that it can be used between any two nodes*
>   - *remove wmf-specific dependencies so that it may be used outside of the org*
>   - *make it work in Labs*
>   - *achieve better code/data separation*
>   - *remove dependency on role::cache::configurat*

> > > >

Jan 5 2015, 6:13 PM

I feel that we need greater clarity about exactly who are we protecting our traffic from and how much effort is appropriate to expend on this goal.

From an article in Ars Technica dated Dec 30 2014 (http://ars.to/1B230yP):

"... in 2010, the NSA had already developed tools to attack the most commonly used VPN encryption schemes: Secure Shell (SSH), Internet Protocol Security (IPSec), and Secure Socket Layer (SSL) encryption."

This article discusses PSK, which we do not use, but also IKE:

"...trying to capture IPSec Internet Key Exchange (IKE) and Encapsulating Security Payload (ESP) traffic during VPN handshakes to help build better attacks."

if that doesn't work, they try:

"...gathering more information on the systems of interest from other data collection sites or doing an end-run by calling on Tailored Access Operations to “create access points” through exploits of one of the endpoints of the VPN connection."

We must assume that this agency is not the only one with such capacity.

My question is: exactly who are we trying to secure our inter-colo communications from, and what is the feasibility of achieving that goal in the face of this information?

My impression is that adding IPsec can only potentially protect us from actors who can gain access to routers along our transit paths and record our traffic but do not have resources to apply the above methods.

• **Gage** closed subtask
Restricted Task as *Resolved*.
Jan 11 2015, 4:13 PM

• **Gage** added a comment.
Jan 12 2015, 4:51 AM

More on the 12/2014 leaked info, from a Libreswan developer: "If you configure your IPsec based VPN properly, you are not affected. Always use Perfect Forward Secrecy and avoid PreSharedKeys.":
https://nohats.ca/wordpress/blog/20
stop-using-ipsec-just-yet/

In Strongswan: "IKEv2 always uses PFS for IKE_SA rekeying whereas for CHILD_SA rekeying PFS is enforced by defining a Diffie-Hellman dhgroup in the esp parameter.":
https://wiki.strongswan.org/projects/
https://wiki.strongswan.org/projects/

esp = <cipher suites>
The notation is encryption-integrity[-dhgroup][-esnmode]
Defaults to aes128-sha1,3des-sha1
As a responder both daemons accept the first supported proposal received from the peer. In order to restrict a responder to only accept specific cipher suites, the strict flag (!, exclamation mark)

Currently configured value: esp=aes256-sha512-modp4096!

Input on cipher suite selection is solicited.

faidon mentioned this in ~~**T86663: Expand HTTP frontend clusters with new hardware**~~. Jan 13 2015, 2:41 PM

Dzahn added a subscriber: **Dzahn**. Jan 20 2015, 7:26 PM

BBlack added a subscriber: **BBlack**. Jan 20 2015, 7:27 PM

chasemp added a project: ~~**Interdatacenter-IPsec**~~.
Jan 20 2015, 7:42 PM

• **Gage** mentioned this in **rOPUP917a7be9e69a: Strongswan: IPsec Puppet module**. Mar 1 2015, 11:19 PM

Jdforrester-WMF added a subscriber: **Jdforrester-WMF**.
Mar 10 2015, 6:50 PM

greg added a subscriber: **greg**.
Mar 11 2015, 2:49 AM

Dzahn awarded a token.
Mar 11 2015, 3:07 AM

• **Gage** closed subtask Restricted Task as *Resolved*.
Mar 13 2015, 5:35 AM

• **Gage** closed subtask Restricted Task as *Resolved*.

BBlack added a subtask: ~~**T96854: Reboot caches for kernel 3.19.6 globally**~~.
Apr 22 2015, 2:30 PM

BBlack added a subtask: ~~**T94417: Fix ipv6 autoconf issues**~~.
Apr 22 2015, 2:35 PM

BBlack added a comment.
Apr 27 2015, 8:05 PM

> Where are we at on this, aside from my blockers for final rollout re: kernel updates + IPv6 SLAAC?

BBlack added a parent task: ~~**T86718: Upgrade eqiad-misc varnish cluster from 2 to 4 systems.**~~.
Apr 27 2015, 8:05 PM

BBlack added a subscriber: **faidon**.

May 3 2015, 11:19 PM

I've been going over the Interdatacenter-IPsec tasks today trying to get a picture of the overall situation and what's blocking various stages of deployment. This is a basic rundown of how I see things now:

I don't think we need or want crypto-traffic-only enforcement at this stage. Let's get this rolled out in a form where we still fall back to working, unencrypted traffic and simply have good monitoring in place that will alert us to this fallback condition. We can explore whether and how we want to force encryption at a later date. It could well be the case that ipsec with hostpair associations is not how we address our traffic crypto problems in the very long term view anyways. What we need now is just basically-reliable protection and alerting.

Tickets that can probably be ignored/dropped for now and not block deployment:

1. **T85823** - firewall rules - see above re: enforcement
2. T85827 - opportunistic encryption - seems dead-for-now upstream, so not really an available option

3. T85822 - restricting crypto to specific ports' traffic - does not seem necessary. The bastions won't be among the hostpairs involved, so SSH via them will always work fine. The traffic we'd want protected is the bulk of the traffic for any given hostpair, so efficiency isn't a big concern here either. If anything, not restricting by-port is a more secure-by-default solution anyways.

Nits that can probably easily be cleaned up / closed / ready:

1. ~~T96111~~ - Previous reauth failure investigation - seems ready to close, modulo ensuring we've discovered/applied sane runtime production values for various related parameters like lifetime and margin.
2. ~~T92604~~ - Rollout plan - seems sane, although the primary ticket text is a bit mixed/dated (we don't have it applied on all esams text caches, for instance, and wouldn't as a first step...). But yes, the general idea here to test on one hostpair only in production and then gradually enable the others is sane.
3. T95373 - Update Puppet CA cert - doesn't seem to be a

true blocker, more like "if we're going to fix this, let's do it now instead of later". Shouldn't be hard, right? If not, let's get it over with. If it is, then let's not block IPSec on it.

4. T88536 - Implement a big IPsec off switch - core script seem to already be merged and presumably basically works? There's a followup commit dating back to ~2w ago with some nits/bugfix traffic, not yet merged. What's stalling on this? https://gerrit.wikimedia.org/

Functional core IPsec things that definitely need to be working for deployment, and may need some serious work-time on them:

1. T92603 - Monitoring - Seems we have some work here, but is missing (in my opinion) "ip xfrm" correlation, plus reviewing for smaller nits and such, and actual testing. Critical due to lack of real traffic enforcement, so that we're aware if things break down.
2. T92602 - Stats traffic protection - Critical IMHO, as we're still leaking way too much information without this. Needs: identify the list of kafka brokers involved, figure out if they're already on jessie or

pre-req for our current working test configs), sort out puppet bits for including them in the configured hostpairs for tier2 DCs as well. If they're not jessie yet, this could be a pretty major holdup. We could go ahead without this initially just to get some protection in place, but we really need this ASAP regardless.

External blockers (not IPSec-specific, but block full production rollout):

1. ~~T94417~~ - Fix ipv6 autoconf issues - @faidon and I should be able to sort this out one way or another before the rest above is done.
2. ~~T96854~~ - cache reboots for kernel updates - We should be able to kick off this process later this week, and thus would expect completion by circa May 22 at the outside? We can overlap this with the first phases of rollout by ensuring we get a few key hosts rebooted early in the process that can be used for the initial production hostpairs.

Is there anything else missing that's not captured in all of the above?

• **Gage** closed subtask
Restricted Task as *Declined*.
May 4 2015, 5:43 PM

• **Gage** added a comment.
May 4 2015, 5:52 PM

Thanks, Brandon. I'll reply in order:

Proposed for ignore/drop:

1. **T85823: IPsec: add firewall r**
   Agreed, we don't need this right now. However I suspect we'll want this someday. Not a blocker. Propose: keep open with lowest priority.
2. {T85827}: Agreed, no movement upstream. It's a nice idea which could have made configuration easier, but we've already done the config work so now this would represent a config change rather than a savings in effort. I've closed it.
3. {T85822}: I opened this per Mark's request but personally I don't think we'll ever need this. The goal was to minimize potential impact of IPsec, but as BBlack has pointed out this is sufficiently taken care of by the hostpairs in use: DNS lookups, SSH from bastions,

etc. will never be affected by IPsec. Propose: close.

Clean up / close / ready:

1. ~~**T96111: Strongswan: secu**~~
   Updated. Need to import Strongswan 5.3.0 into WMF apt repo. Need to determine appropriate values for lifetime and margin.
2. ~~**T92604: IPSec: roll-out pl**~~
   Updated. It seems we're in agreement to try a pair of upload hosts first.
3. {T95373}: I removed Interdatacenter-IPsec tag from this, but now I'm having second thoughts. It means replacing the puppet cert on every host, because they're signed with the CA cert which needs replacement. Not hard, but also not trivial. If we do this after IPsec roll-out, it /should/ be as simple as running puppet to copy the new keys into /etc/ipsec.d/cacerts/ and restarting Strongswan.
4. ~~**T88536: Implement a big**~~
   Revised patch uploaded this morning. Needs review but according to me it's bug-free & ready.

Core requirements:

1. ~~**T92603: Monitor IPsec sta**~~
   Revised patch uploaded this

xfrm' checking and addresses syntax issues. Review requested.

2. **~~T92602: Secure inter-datacer~~** I agree that this is important. Kafka brokers are still on Precise, so they will need to be reinstalled. I'll talk to Otto about this.

External blockers:

1. **~~T94417: Fix ipv6 autoconf is~~** I've tested & given my feedback in support of the token-based approach. Seems like we're waiting on feedback from Paravoid.
2. **~~T96854: Reboot caches for k~~** This is BBlack & Moritz's issue, I agree with the plan to overlap with first phases of rollout. We need at least 3.19.3, which works with the current plan to deploy 3.19.6.

I'm not aware of any other related issues.

• **Gage** closed subtask Restricted Task as *Declined*.
May 6 2015, 5:53 PM

• **Gage** removed a subtask: **~~T85823: IPsec: add firewall rules~~**.

BBlack closed subtask **~~T96854: Reboot caches for kernel 3.19.6 globally~~** as *Resolved*.

May 26 2015, 12:47 PM

BBlack closed subtask ~~**T94417: Fix ipv6 autoconf issues**~~ as *Resolved*.

May 28 2015, 6:53 PM

BBlack removed a parent task: ~~**T86718: Upgrade eqiad-misc varnish cluster from 2 to 4 systems.**~~. Jun 4 2015, 12:01 AM

BBlack added a parent task: ~~**T101339: Expand misc cluster into cache PoPs**~~.

Jun 4 2015, 12:05 AM

BBlack added a subtask: ~~**T92604: IPSec: roll-out plan**~~.

Jul 29 2015, 1:27 AM

Restricted Application added a subscriber: **Matanya**. · View Herald Transcript

Jul 29 2015, 1:27 AM

BBlack mentioned this in **rOPUPc86d5d45df63: enable ipsec for all codfw caches**.

Jul 30 2015, 10:16 PM

BBlack mentioned this in **rOPUP651418a26dca: enable ipsec for half eqiad text caches**.

BBlack mentioned this in **rOPUP390b3d7b7047: enable ipsec for all eqiad text caches**.

BBlack closed subtask ~~**T92604: IPSec: roll-out plan**~~ as *Resolved*.

Aug 3 2015, 3:56 PM

BBlack added a subtask: ~~**T92602: Secure inter-datacenter web request log (Kafka) traffic**~~.

Aug 3 2015, 4:06 PM

BBlack added a comment.

Aug 3 2015, 4:09 PM

So, the basic cache<->cache work for tier2 is complete and functioning in practice (modulo ongoing operational improvements). We're still missing protection of other traffic (critically, kafka data, blocker added to previously merely referenced ticket), and we still have no answer for the traffic that crosses DCs through an LVS (critically in the near future: codfw caches -> eqiad appservers. Beyond that, it is desirable to let tier2-frontend caches bypass flowing through tier2-backend+tier1-backend for fixed "pass" traffic, but we're not there yet and this basically blocks it.

BBlack mentioned this in ~~**T110065: Switch codfw caches to tier2, begin**~~

~~**pushing some traffic through them to test**~~.

Aug 24 2015, 5:02 PM

BBlack removed a subtask: ~~**T92602: Secure inter-datacenter web request log (Kafka) traffic**~~.

Aug 27 2015, 3:01 AM

BBlack added a project: **Traffic**.

BBlack closed this task as *Resolved*.

Aug 27 2015, 3:29 AM

I split off the last blocker as a separate Traffic-tagged ticket. It's important, but there's no clear priority vs other projects, and we may solve it without IPSec anyways. The rest of the work here has been functional for a while and it's time for this long-standing meta-task to die.

BBlack moved this task from **Triage** to ~~**Done**~~ on the **Traffic** board. Sep 22 2015, 1:57 PM

faidon changed the visibility from "**WMF-NDA** (Project)" to "Public (No Login Required)".

Dec 13 2017, 5:09 PM

faidon changed the edit policy from "**WMF-NDA** (Project)" to "All Users".

USCA4 Appeal: 20-1191 Doc: 18-3 Filed: 07/01/2020 Pg: 486 of 529

Log In to Comment

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

Plaintiff's Exhibit 40

Job descriptions/Traffic Security Engineer

< Job descriptions

Summary

We are looking for an Operations Engineer to join our Technical Operations team. Would you like to join the highly dynamic team that is responsible for the reliability and performance of a global top-10 website, Wikipedia?

The Technical Operations team has a very broad range of shared responsibilities. The team is globally distributed, working remotely with each other in a highly collaborative and consensus-oriented fashion. We only write and only use Open Source code wherever possible and we do the vast majority of our work in public view.

This Traffic Security position focuses more-specifically on the Security and Privacy responsibilities of our Traffic team within Operations. The Traffic team runs a private and privacy-protecting global CDN for Wikipedia and related sister projects. One of the key responsibilities of this position will be technical stewardship of our TLS termination for users at the edges of our network. We're passionate about protecting the privacy of our users against mass surveillance and manipulation, and we expect you to share that passion. If the word "ChaCha" doesn't make you think of dancing first, you might be the person we're looking for!

We'd like you to do these things:

- Protect our users' reading and editing habits from mass surveillance
- Keep our TLS infrastructure up to date in the face of evolving threats
- Keep track of the ever-changing landscape of browsers and other UAs
- Analyze and optimize our edge software infrastructure to enhance our users' experiences
- Assess and deploy newer protocols, technologies, and software as their time becomes ripe
- Deprecate older ones in a timely manner while balancing the needs of legacy clients
- Reactively respond to, and proactively engineer against, DDoS and other attacks
- Analyze and advise on application-layer security issues exposed over HTTPS
- Other related Traffic and Security/Privacy work as required

Experience we'd like you to bring to the table:

- A deep and current understanding of TLS, HTTP[S], TCP/IP, DNS, and other related protocols
- Hands-on experience working with TLS libraries and HTTP server software configuration
- A working knowledge of modern cryptography from a systems engineering point of view
- Experience working on general infrastructure and application-layer security issues
- Experience with Open Source operations tooling for configuration management, orchestration, and monitoring.
- Experience working on Open Source operations infrastructure in general
- Bachelor's degree or the equivalent in related work experience

And it would be even more awesome if you have any of these:

- Experience operating TLS-terminating reverse proxy servers at global scale
- Experience operating large web properties at a global scale
- Programmer experience writing and/or modifying network daemons and/or libraries in languages such as C, C++, Go, Python, and/or Rust

- Some knowledge of Linux IPVS load-balancing
- Some knowledge of global IP routing
- Some knowledge of HTTP caching and related CDN technologies

Some public links on the current state of our TLS termination you might be interested in:

https://grafana.wikimedia.org/dashboard/db/tls-ciphers https://www.ssllabs.com/ssltest/analyze.html?d=en.wikipedia.org https://wikitech.wikimedia.org/wiki/HTTPS

Retrieved from "https://office.wikimedia.org/w/index.php?title=Job_descriptions/Traffic_Security_Engineer&oldid=223926"

This page was last edited on 9 January 2018, at 08:10.

The contents of this **Office Wiki** are confidential. Only users that have signed the Wikimedia Foundation's Confidentiality Agreement are authorized to have access.

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

Plaintiff's Exhibit 41

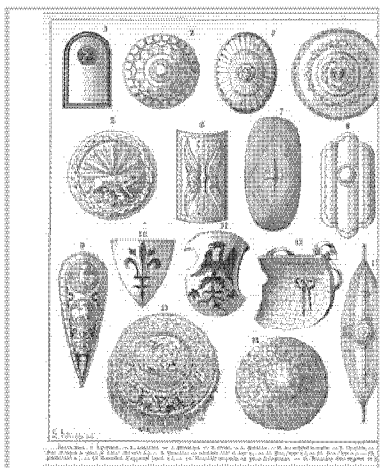
FREE CULTURE, FREE KNOWLEDGE, LEGAL, WIKIPEDIA

A Proposal for Wikimedia's New Privacy Policy and Data Retention Guidelines

By Michelle Paulson, Wikimedia Foundation
February 14th, 2014

Shields, circa 1870 Privacy policies play a vital role in protecting the privacy of users. At the Wikimedia Foundation, our Privacy Policy is particularly important to us, because it is a key way we protect our users and reflect their values. It also has a broad impact, because it protects and governs the information of over twenty million registered users and 490 million monthly unique visitors. Our current Privacy Policy was approved by the Wikimedia Board of Trustees in October 2008 and has not been updated since. Given the growing concern over privacy, especially on the internet, it is important

Privacy policies play a vital role in protecting the privacy of users. At the Wikimedia Foundation, our Privacy Policy is particularly important to us, because it is a key way we protect our users and reflect their values. It also has a broad impact, because it protects and governs the information of over twenty million registered users and 490 million monthly unique visitors.


Shields, circa 1870

Our current Privacy Policy was approved by the Wikimedia Board of Trustees in October 2008 and has not been updated since. Given the growing concern over privacy, especially on the internet, it is important to have an updated policy which reflects both technological advances and the evolving legal issues surrounding new technology.

So, almost eight months ago, we started a conversation with the Wikimedia community about key privacy issues. Based on that conversation, we crafted a new draft Privacy Policy and introduced it to the community for feedback about five months ago. And, thanks to that feedback, we created and discussed Wikimedia's first Data Retention Guidelines. Today, we are closing the community consultations on the new draft Privacy Policy and Data Retention Guidelines. [1]

The new proposed Privacy Policy will now be presented to the Wikimedia Board of Trustees for review before its next meeting in April 2014. If approved, it will replace the 2008 Privacy Policy.

GET CONNECTED

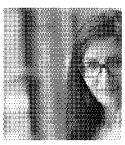
GET OUR EMAIL UPDATES

Your email address

Subscribe

MEET OUR COMMUNITY


The one-man band writing the history of Nigerian cinema into Wikipedia


Wikipedia is a to "plant and harvest" free knowledge: Ar Aghayan

More Community Profiles

MOST VIEWED THIS MONTH

'Monumental' winners from th world's largest photo contest showcase history and heritage
The top fifteen images from Wiki...

Türkiye'den Vikipedi'ye erişim engeli halen devam ediyor
Vikipedi'nin tüm dil sürümleri, Nisan ayını

New monthly dataset shows w people fall into Wikipedia rabl holes
The Wikimedia Foundation's Analytics te

ARCHIVES

FEBRUARY 2018

JANUARY 2018

We would like to thank the many community members who participated in the discussions. The new proposed Privacy Policy and Data Retention Guidelines would not be what they are today without your help. (You can actually see the changes to the drafts in the Policy's and Guidelines' wiki revision histories that happened as a result of your feedback!) We received hundreds of questions, comments, and suggestions. In fact, the discussion on the Privacy Policy, along with the related Data Retention Guidelines and Access to Nonpublic Information Policy (whose consultation is also closing today) totaled approximately 195,000 words, making it longer than the Fellowship of the Ring! Together, we have created a transparent Privacy Policy draft that reflects our community's values.

We'd like to go over some of the ways that our new proposed Privacy Policy differs from our old Privacy Policy (the "2008 Policy"). One thing that has not changed is our goal of collecting as little information as possible, but we have made a wide variety of improvements to strengthen our commitment to users, including:

- **More detail and transparency.** Our old Privacy Policy did not provide a great deal of specific information about what kind of data we collected or how we collected and used it. The new proposed Privacy Policy and Data Retention Guidelines explain these points in detail, so that users have a better understanding about their privacy on Wikimedia Projects.
- **The permitted use of different types of technologies.** The 2008 Policy covered IP information and cookies. The new proposed Policy, on the other hand, explains how information is collected from mobile devices, tracking pixels, JavaScript, and "locally stored data" technologies, so that we can improve the Projects.
- **Never selling user data.** The 2008 Policy doesn't mention this. While long-term editors and community members understand that selling data is against our ethos, newcomers have no way of knowing how our Projects are different from most other websites unless we tell them. The new proposed Policy spells out that we would never sell or rent their data or use it to sell them anything.
- **New glossary and FAQ.** The new proposed Policy includes a glossary that helps users familiarize themselves with wonky technical terms such as API and metadata. It also includes an FAQ to help users understand details about Wikimedia Sites, our privacy practices, and data collection technologies. For example, the FAQ provides examples of the types of technology we use to collect data, and explains to users how they can limit some of the information that is collected about them.
- **Inclusion of new activities.** We started new projects and features (like notifications, surveys, and feedback tools) after the adoption of the old Policy, so unsurprisingly the old Policy doesn't address them. The new proposed Policy explains how notifications are used and how you can opt out as well as how we may use information collected in surveys.
- **Limited data sharing.** The old Policy narrowly states that user passwords and cookies shouldn't be disclosed except as required by law, but doesn't specify how other data may be shared. The new proposed Policy expressly lists the limited ways in which all data may shared, including with our essential volunteers. It permits providing non-personal data to researchers who can share their findings with our community so that we can understand the Projects and make them better. We have also added a Subpoena FAQ as a resource for users to learn about subpoenas generally and what they can do in the unlikely event their information is subject to a subpoena.
- **Scope of policy.** The 2008 Policy states its scope in general terms, which could be confusing or ambiguous. The new proposed Policy explains in detail when the Policy does and doesn't apply.
- **New Data Retention Guidelines.** While not formally part of the new proposed Privacy Policy, for the first time, we have a formal document, drafted in close consultation with engineering, outlining what our data retention practices are and should be. In creating these Guidelines, we tried to be as thorough as possible in specifying how long particular types of personal information will be kept.

The proposed Privacy Policy and the Data Retention Guidelines are the result of an organization-wide effort — staff from many departments helped us create these documents, and we would like to thank everyone who participated. In particular, we would like to thank Erik Möller and the entire engineering team for their continued support and participation throughout this process.

Michelle Paulson, Legal Counsel

Geoff Brigham, General Counsel

DECEMBER 2017

NOVEMBER 2017

OCTOBER 2017

OLDER POSTS 26

WORK AT WIKIMEDIA

Work with the foundation that supports W and its sister projects around the world. A and join us

1. Although we are closing the formal community consultation on the Data Retention Guidelines, we welcome community members to continue the discussion. The Guidelines differ from policies in that they do not require approval from the Board to be implemented and can be continually updated and improved. We intend for these Guidelines to evolve and expand as time goes on.

* So many people helped us on this project. Special thanks go to Toby Negrin, Luis Villa, Dario Taraborelli, Roshni Patel, Megumi Yukie, James Alexander, and Jorge Vargas, without whom these privacy documents and consultations would not have been possible.

25 Comments on A Proposal for Wikimedia's New Privacy Policy and Data Retention Guidelines

Sabrina Vizcaino 4 years

Valoro el hecho de querer aplicar una política de privacidad mas rígida pues muchos de los documentos de wikipedia contienen errores provocados por los mismos usuarios, aun así, creo que las opiniones de usuarios que si tengan conocimiento pleno de un tema en particular y observando su nivel de preparación académico, deberían de ser tomadas en cuenta para la perfección del documento sin que el mismo sea alterado directamente

Share

Francisco 4 years

Un saludo cordial.
Decir que no entiendo Ingles, por lo tanto no se en que términos y condiciones va a cambiar la política de privacidad de vuestra pagina WEB, a través de la encuesta realizada, es decir que querria que se tradujera tambien al Castellano o Español. At..WIKIPEDIA……GRACIAS

Share

clarence nalls 4 years

I am concerned with googles practice of listing information regarding individuals that may not be true which could damage ones reputation. Such as, information regarding disciplinary proceeding regarding an attorney that my be false without giving the affected person an opportunity to respond. Such practice should be stopped.

Share

Doctor 4 years

Some of us appreciate you all taking a clear, deliberate, and most importantly accountable policy when it comes to user security. This place in internet history is an especially murky and uncertain one, where the Utopian fools, cowboys, and salesmen have rather unflatteringly metastasised into mutually assured, multiplicitous beast. Seeded in the psychology what used to be just one of many search engines. Now obsessed with a subjective definition (and subsequent dominion) of all topology of the landscape, (to the point where many people will never understand or see beyond what has been framed for them – hypothetically: You were a Web Host or Small Business, and were refused a listing by Google at the behest of an influential agency or party. You made the robots.txt list- For a for all intents and purposes: You Do Not Exist – and you will struggle to posit a public reality the contrary) This omnivore in altruist's clothes has created and refined both models of data aggregation, user targeted advertising and especially good at expertly deflecting any criticisms of violations of their user rights (picture of Magna Carta for internet missing : that's a 404)implicit in their systems. (the same thing that seems to allow repeated gross ethical misconduct: lack of precedent or legislation makes all rights simply implied.) It is the emulation of their corporate dollar driven profiling of the ontological and semantic web, now used for and

by both the social networks (see:The flailing minutiae / cult of personality bubble) .and corporate modern web. And it is the progenitor of the worst of it. The once uninitiated NSA, now the peak of it's crypto-fascist dream. So thanks for drawing a line in the sand. It's amazing that Wikipedia still has not caved in/"Been acquired" there aren't many institutions with ethics left intact once they reach your place. Thank you. Some of us see what you are doing, and some of us are listening.

Share

Ralph Dratman 4 years

With respect to the likelihood or otherwise of a subpoena being issued against user information stored by Wikipedia, your assertion that such was "unlikely" was, I must assume, referring to the probability that any given specific user (for example, the reader of this document) would ever be subject to such. On the other hand, I'd guess the aggregate probability that some one or more users among all the wikipedia users will at some future time be subject to such subpoena is not negligible.

Share

lola 4 years

Gracias por avisar

Share

Jonathan Pineda 4 years

Thank you.

Share

Steve 4 years

Wikipedia needs a better policy as regards transparency regarding the actions of its administrators. Some may be over zealous in some regards. It might be helpful for users to see statistics on administrative actions and be able to vote for which ones they value most and least with the objective of setting administrative limits, so many per week per administrator on the ones valued least.

Share

Sxxxx Wxxxx 4 years

I'm disappointed I didn't come across this sooner. It would have been the perfect opportunity to ONCE AGAIN voice my concern and disappointment that Wiki has gone the way of our democracy; at times to the highest bidder. Suggesting a few more fixes to cure their edit process might have helped the +90% of Wikipedia that serves its purpose…

As central a resource as Wiki is, it's not quite the incredible, compounding central database it could have been. Whether it's a policy issue or some short-coming of all wiki-s, it seems when subsequent corrections/edits don't sit well with a special interest or a corporate sponsor —- even if properly annotated and referenced — changes can go missing, routinely, again and again, over months, continually, as if a well funded machine was able to maintain their talking points over the balanced and unbiased maintenance of information. All while Wikipedia sat by and did little to nothing. Public safety issues or other concerns aside, this is sides taking plain and simple, of which Wikipedia unwittingly or not has become a tool and not the right side of history we'd all expect.

It's been years since I've bothered editing, or donating (since), yet the in-depth and unbiased exposé of even the issues of plastics, Excitotoxins (MSG, Aspartame, etc), GMO, the toxic adjuvants in vaccines, and a whole host of other now common "controversies" is evidentiary and still up for grabs or a slanted treatment. Unfortunately and because of this, and completely contrary to what I'd hoped; I have to wonder

their intentions and their charitable status, while ostensibly at times a special interest driven mouthpiece for corporate sponsors…

Share

Trevor Webb 4 years

In reference to comment 13, I hope there is still some facility for correcting wicki entries. For example I am an aviation historian with 50 years experience and a masters degree and often find, usually minor, errors.

Share

levi van dijk 4 years

if you want details to be safe use pen , paper and mechanical storage. people are too lazy to "spy" or forcefully record information in books and literal files. i personally dont trust any digital information to be truly "private". im an industrialist who prefers mechanical contraptions more so than electronically functioning technology.

i guess metaphorically when referring to technology i prefer the "indomitable divide" to the "cutting edge".

Share

John Couch 4 years

Julie Krauel – the reason your school won't allow Wikipedia or any other web source to to be used is that they are not original data. The thing that is great about Wikipedia is that the reputable articles have footnotes. Go to them for your sources.

Share

Julie krauel 4 years

Why won't school allow this site for reports?

Share

Julie krauel 4 years

Mr. Crout,
What do you mean?
Jkrauel

Share

Julie krauel 4 years

Let me explain myself. I am learning more & more about the web. Especially since after being hacked of all my personal info in Oct. 13 I don't know who to.hold responsible? I was simply now making a comment about Google+ note allowing you to take your name off of all"public just profile." When you have to sign up to get better apps. I would like all my info private…thank you. I will show my first name.. My kids Uuse your site for reports but now are banned to get any info. From you for reports. Why? I was wondering if you could tell me? Also the other apps. I. Meantioned was Google Hangouts where up to get10 people can join in. They don't mention and listen to your calls sms as invisible??? If I wanted to spy on someone I would install that app. I was wondering not bragging on Google I was wondering if there were ways around having your info private but when it says it will be. Just as aiki said my email was kept private? WIKI not very trustworthy afterall. Great comment to make me look bad when I was wondering simply asking for help. You DEFINITELY DO NEED A NEW PRIVACY POLICY! ASAP!

Share

Julie krauel 4 years

I am not trusting of this site automatically showing my info as public just for signing in. Google makes you pretty much have too to get other apps free. Is there a way you can avoid this? I made all private but I know a lot of people that do not know about that site and handouts with invisible listeners on your calls sms beware to all these apps are spyware & sneaky!:-*

Share

James Carr 4 years

The main reason I use wikimedia is for educating myself on different subjects ! I don't use it very often,but when I do you seem to have the most useful facts on the ole inner web . Today I was searching for some army & navy info on my Uncle and Dad .I have a few unanswered questions and they're both passed on,so it being Memorial Day I thought I would try and get a little information. But with everything going on in this world of ours this day and time you can't be to careful!!! I understand completely. Thank you,I think wikimedia is doing a great job !!!

Share

Javier ezequiel grob 4 years

Entiendo que Wikimedia sea mejor que Wikipedia, si seria mas mejor que sea privado y no en publico. Servira un mejor ejemplo que tenga mejor información en Wikimedia que en Wikipedia y que tenga los mismos idiomas o mas mejores y nuevos idiomas que los idiomas anteriores. Puede que eso sirva como un mejor ejemplo de transparencia para que todos en los países del mundo en Sudamérica, Norteamérica, Europa, África, Asia y Oceanía (Australia). Puede que sea un mejor detalle como que este Wikimedia permita que la organización muestre el verdadero respecto hacia todos los clientes de todo el mundo y que nosotros podamos valorarlo que su privacidad pueda haber sido de una vez por todas por genuina, pero ahora es la retorica y espero que esto signifique que no esto se pueda cambiar o que esto pueda alterar toda la información proporcionada por el wikimedia.

Share

NESTOR SANTIN VELAZQUEZ 4 years

La trascendencia sin precedente de este proyecto es patente. Es como un sueño de la alfombra voladora, pero en el terreno de la ciencia y la técnica. El carácter multidisciplinario y plural, y al mismo tiempo objetivo en la construcción de contenidos no debe ser afectado, idealmente. Tampoco el carácter gratuito (No profit)aunque yo he colaborado modestamente (minúsculas cantidades de dinero) y estoy dispuesto a seguir colaborando, según mis posibilidades. Este proyecto ya es fundamental para la humanidad. Me gustaría colaborar con información de mi región y país, pero lo haría sólo en temas en los que pudiera aportar algo nuevo o desconocido. Mientras esto se materializa, gracias, gracias, gracias.

Share

Dawn Tuskey 4 years

Wow. Impressive. Wikimedia is leading by example. Never selling the little bit of info I share & you collect is a big one to me. It's gotten to the point where I'm wondering if & how I should copyright & trademark my name & other personal info.

Share

MORE COMMENTS

Comments are closed.

WIKIMEDIA FOUNDATION

The Wikimedia Foundation, Inc is a nonprofit charitable organization dedicated to encouraging the growth, development and distribution of free, multilingual content, and to providing the full content of these wiki-based projects to the public free of charge. Get Involved | Log In

WIKIMEDIA PROJECTS

The Wikimedia Foundation operates some of the largest collaboratively edited reference projects in the world.

WIKIPEDIA	COMMONS	MEDIAWIKI	WIKIBOOKS
WIKIDATA	WIKINEWS	WIKIQUOTE	WIKISOURCE
WIKISPECIES	WIKIVERSITY	WIKIVOYAGE	WIKTIONARY

WIKIMEDIA MOVEMENT AFFILIATES

The Wikimedia projects have an international scope, and the Wikimedia movement ha already made a significant impact throughout the world. To continue this success on a organizational level, Wikimedia is building an international network of associated organizations.

WIKIMEDIA CHAPTERS THEMATIC ORGANIZATIONS WIKIMEDIA USER GROUPS

This work is licensed under a Creative Commons Attribution 3.0 unported license. Some images under CC BY-SA.
Read our Terms of Use and Privacy policy. | Powered by WordPress.com VIP

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

Plaintiff's Exhibit 42

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

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

Plaintiff's Exhibit 43

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

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

Plaintiff's Exhibit 44

wikimedia / analytics-reportcard-data

Branch: master ▾ analytics-reportcard-data / datafiles / rc_comscore_region_uv.csv Find file Copy path

milimetric Update data through December a0ee5a3 on Dec 21, 2015

4 contributors

183 lines (182 sloc) 7.57 KB

We can make this file beautiful and searchable if this error is corrected: Unquoted fields do not allow \r or \n (line 2).

```
date,World
,China,Europe,India,Latin-America,Middle-East/Africa,North-America,Asia Pacific
2007/12/01,226119000
,469000,84703000,4758000,19063000,10828000,57630000,53895000
2008/01/01,242554000
,581000,91036000,5138000,18341000,11549000,61664000,59964000
2008/02/01,240754000
,695000,87975000,5065000,20286000,11327000,61218000,59948000
2008/03/01,256061000
,669000,92283000,5200000,24542000,13337000,63518000,62380000
2008/04/01,261414000
,2288000,93642000,5079000,26347000,13634000,63827000,63963000
2008/05/01,263120000
,994000,95234000,5264000,27002000,14139000,63186000,63560000
2008/06/01,251502000
,958000,89427000,5979000,26099000,11941000,58272000,65764000
2008/07/01,244326000
,232000,86905000,5720000,23220000,11016000,57347000,65838000
2008/08/01,248539000
,1382000,83931000,6217000,26847000,11371000,59494000,66895000
2008/09/01,272109000
,2735000,98304000,6025000,28886000,12553000,64075000,68291000
2008/10/01,277208000
,2037000,102955000,5799000,27974000,13790000,66785000,65703000
2008/11/01,280969000
,2185000,106199000,6286000,27416000,13850000,65133000,68371000
2008/12/01,272998000
,2286000,105318000,6421000,22769000,15103000,63782000,66026000
2009/01/01,289811000
,1825000,112449000,6764000,22558000,15630000,67971000,71203000
2009/02/01,300751000
,2002000,117828000,6587000,27440000,18765000,65855000,70862000
2009/03/01,327148000
,2752000,126474000,7014000,34229000,21558000,66878000,78009000
2009/04/01,320043000
,3115000,119578000,6807000,33400000,20133000,70908000,76024000
2009/05/01,317255000
,2936000,118874000,7168000,33870000,19529000,69387000,75595000
2009/06/01,302940000
,4566000,112270000,7522000,33263000,16489000,64678000,76239000
2009/07/01,295484000
,3839000,108552000,7908000,29298000,16502000,66142000,74990000
2009/08/01,307641000
,3547000,111190000,8398000,33186000,17816000,68084000,77365000
2009/09/01,325998000
,2882000,123062000,8480000,35264000,18063000,71661000,77948000
2009/10/01,344563000
,3702000,128647000,9287000,36440000,22353000,73452000,83671000
2009/11/01,345805000
,3718000,129798000,9437000,36495000,22083000,75050000,82379000
2009/12/01,347020000
,3657000,129763000,9696000,31391000,24058000,77607000,84201000
```

```
2010/01/01,364719000
,3351000,136935000,10216000,32834000,23411000,82489000,89049000
2010/02/01,345218000
,2935000,133807000,9865000,36414000,21680000,80940000,72378000
2010/03/01,370744000
,3443000,140834000,10516000,43574000,24962000,83696000,77678000
2010/04/01,374846000
,4081000,144087000,10923000,44286000,25146000,83792000,77535000
2010/05/01,388932000
,2700000,150313000,11675000,45790000,26399000,85929000,80502000
2010/06/01,379112000
,2613000,151013000,12373000,43826000,23611000,80393000,80269000
2010/07/01,360225000
,2536000,138975000,12828000,38111000,22991000,79888000,80260000
2010/08/01,373392000
,2829000,140560000,13187000,42303000,26220000,81295000,83015000
2010/09/01,398178000
,3181000,155438000,13433000,45265000,28749000,85606000,83119000
2010/10/01,408350000
,3156000,159384000,13674000,45152000,33049000,87359000,83406000
2010/11/01,410816000
,3108000,165020000,13614000,46617000,30711000,85732000,82736000
2010/12/01,395472000
,3372000,157837000,14004000,38738000,30852000,87087000,80958000
2011/01/01,413957000
,3048000,168571000,15067000,39446000,32113000,88233000,85593000
2011/02/01,379415000
,2664000,150775000,12960000,41411000,29722000,80038000,77468000
2011/03/01,400011000
,2854000,156913000,13011000,47583000,32599000,81918000,80997000
2011/04/01,380716000
,2866000,149211000,12801000,45108000,30272000,78234000,77891000
2011/05/01,411061000
,3492000,161311000,13701000,49095000,33908000,82081000,84666000
2011/06/01,399362000
,3960000,153883000,14163000,47203000,30985000,80753000,86539000
2011/07/01,393543000
,4814000,146724000,14979000,42700000,29882000,83859000,90378000
2011/08/01,422779000
,5163000,152109000,15944000,52983000,31749000,88277000,97661000
2011/09/01,454529000
,5709000,166505000,16180000,56613000,35877000,93193000,102341000
2011/10/01,476627000
,7386000,176918000,16019000,57210000,40119000,96252000,106128000
2011/11/01,474723000
,7355000,178580000,16425000,56544000,39614000,94689000,105296000
2011/12/01,457063000
,8803000,173496000,16425000,45235000,40068000,94413000,103851000
2012/01/01,482157000
,8766000,184668000,17205000,47386000,42097000,99821000,108186000
2012/02/01,475699000
,7886000,179385000,18771000,51425000,41056000,98049000,105783000
2012/03/01,489402000
,9249000,180827000,19402000,58584000,42081000,97001000,110909000
2012/04/01,473380000
,6666000,176376000,18688000,55227000,40589000,96664000,104524000
2012/05/01,492393000
,5917000,185344000,20016000,58825000,42759000,97378000,108087000
2012/06/01,469644000
,5890000,174151000,21031000,54654000,39560000,93676000,107603000
2012/07/01,451821000
,5761000,163811000,21905000,49387000,35788000,94146000,108690000
2012/08/01,456255000
,5602000,163167000,22027000,52510000,36327000,95824000,108428000
2012/09/01,474864000
,4922000,175027000,21853000,54499000,38445000,98992000,107902000
2012/10/01,488364000
```

```
,4965000,183372000,22749000,55850000,40977000,100152000,108013000
2012/11/01,484489000
,4866000,184660000,22191000,54874000,41530000,97462000,105964000
2012/12/01,472552000
,4457000,183718000,23339000,45777000,40802000,96966000,105288000
2013/01/01,488473000
,4194000,192293000,24140000,47216000,40429000,99277000,109258000
2013/02/01,482999000
,3218000,182809000,23104000,60701000,37906000,96653000,104931000
2013/03/01,517610000
,4608000,193348000,24934000,68711000,41553000,100735000,113263000
2013/04/01,516749000
,7412000,190229000,24889000,69779000,41062000,100633000,115045000
2013/05/01,521767000
,8173000,192353000,25892000,69932000,41620000,98666000,119197000
2013/06/01,499578000
,7265000,182455000,26861000,68162000,38842000,92442000,117677000
2013/07/01,492107000
,7996000,176767000,28658000,61155000,37774000,95094000,121316000
2013/08/01,496875000
,7828000,176114000,28286000,67071000,38812000,94693000,120185000
2013/09/01,505904000
,6147000,184950000,27181000,68179000,39522000,96520000,116734000
2013/10/01,530471000
,7900000,195496000,28677000,72075000,42520000,99543000,120838000
2013/11/01,532699000
,8437000,202097000,28160000,70864000,44193000,96223000,119321000
2013/12/01,490200000
,8684000,190982000,27254000,54761000,41467000,89238000,113753000
2014/01/01,495362000
,7188000,199883000,27132000,54583000,41828000,85809000,113260000
2014/02/01,474139000
,7981000,187029000,24917000,59520000,40603000,79780000,107207000
2014/03/01,495184000
,11491000,191667000,25083000,66497000,43485000,80119000,113416000
2014/04/01,465494000
,10378000,180168000,23238000,63455000,40949000,73296000,107626000
2014/05/01,468740000
,10617000,180746000,23524000,66801000,42151000,69452000,109591000
2014/06/01,431791000
,9408000,163846000,24116000,60494000,36908000,63512000,107030000
2014/07/01,412877000
,10797000,154793000,23374000,54275000,32599000,64039000,107170000
2014/08/01,418149000
,8647000,151888000,22309000,57595000,33059000,69723000,105884000
2014/09/01,440710000
,7864000,163573000,21728000,62749000,34151000,74056000,106181000
2014/10/01,459745000
,7706000,174682000,21563000,60589000,38294000,79394000,106785000
2014/11/01,457030000
,5174000,175164000,21972000,59851000,40539000,76913000,104562000
2014/12/01,446656000
,6756000,173737000,22256000,48868000,41370000,79109000,103572000
2015/01/01,455678000
,6981000,177476000,22850000,48760000,41089000,81799000,106554000
2015/02/01,437387000
,5480000,166126000,21435000,53495000,40387000,78353000,99026000
2015/03/01,453097000
,6893000,163025000,21807000,61428000,42202000,81771000,104671000
2015/04/01,439030000
,6330000,153727000,21774000,62000000,43221000,78604000,101478000
2015/05/01,430536000
,4625000,152529000,21250000,61372000,41499000,77758000,97379000
```

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

Plaintiff's Exhibit 45

IMMEDIATE RELEASE

NSA Stops Certain Section 702 "Upstream" Activities

Press Operations

Release No: PA-014-18
April 28, 2017

Since 2008, the National Security Agency (NSA) and other members of the U.S. Intelligence Community have relied on Section 702 of the Foreign Intelligence Surveillance Act (FISA) to conduct surveillance on specific foreign targets located outside the United States to acquire critical intelligence on issues ranging from international terrorism to cybersecurity. After a comprehensive review of mission needs, current technological constraints, United States person privacy interests, and certain difficulties in implementation, NSA has decided to stop some of its activities conducted under Section 702.

While the Foreign Intelligence Surveillance Court (FISC) was considering the government's annual application to renew the Section 702 certifications, NSA reported several earlier, inadvertent compliance incidents related to queries involving U.S. person information in 702 "upstream" internet collection. Although the incidents were not willful, NSA was required to, and did, report them to both Congress and the FISC. The court issued two extensions of the government's renewal application in order to receive additional information from the government about this issue and the government's plan to resolve it. The previous year's certifications remained in effect during these extension periods.

During the extension period, NSA undertook a broad review of its Section 702 program. Under Section 702, NSA collects internet communications in two ways: "downstream" (previously referred to as PRISM) and "upstream." Under downstream collection, NSA acquires communications "to or from" a Section 702 selector (such as an email address). Under upstream collection, NSA acquires communications "to, from, or about" a Section 702 selector. An example of an "about" email communication is one that includes the targeted email address in the text or body of the email, even though the email is between two persons who are not themselves targets. The independent Privacy and Civil Liberties Oversight Board described these collection methods in an exhaustive report published in 2014.

After considerable evaluation of the program and available technology, NSA has decided that its Section 702 foreign intelligence surveillance activities will no longer include any upstream internet communications that are solely "about" a foreign

intelligence target. Instead, this surveillance will now be limited to only those communications that are directly "to" or "from" a foreign intelligence target. These changes are designed to retain the upstream collection that provides the greatest value to national security while reducing the likelihood that NSA will acquire communications of U.S. persons or others who are not in direct contact with one of the Agency's foreign intelligence targets.

In addition, as part of this curtailment, NSA will delete the vast majority of previously acquired upstream internet communications as soon as practicable.

NSA previously reported that, because of the limits of its current technology, it is unable to completely eliminate "about" communications from its upstream 702 collection without also excluding some of the relevant communications directly "to or from" its foreign intelligence targets. That limitation remains even today. Nonetheless, NSA has determined that in light of the factors noted, this change is a responsible and careful approach at this time.

After reviewing amended Section 702 certifications and NSA procedures that implement these changes, the FISC recently issued an opinion and order, approving the renewal certifications and use of procedures, which authorize this narrowed form of Section 702 upstream internet collection. A declassification review of the FISC's opinion and order, and the related targeting and minimization procedures, is underway.

The National Security Agency works tirelessly around the world to help keep the nation safe. We have a solemn responsibility and commitment to do this work exactly right. When incidents occur, we immediately report them to oversight bodies and develop appropriate solutions. We never stop putting improvements in place while carrying out our critical mission.